example 512 bits in comparison with 768 bits. shorter than the fact that a modulus at the level of the proving entity can be work load of the checking entity fundamentally, apart from possible to use the Chinese remainder technique to reduce a module belonging to the proving entity, which makes work loads of the proving entity, which does not change accredited entities is not obligatory. One can use GQ1 with However, the hierarchy of keys between an authority a modulus at the level of the authority, for the the

S

modulus, why call on an RSA digital signature mechanism?? When the entity knows the prime factors of its own

10

often as needed. The security of the GQ2 protocol is equivalent which therefore remains secret, so as to be able to be used as own modulus and this proof does not reveal the breakdown proving entity demonstrates knowledge of a breakdown of its signature". The aim of GQ2 is to reduce work loads, not GQ2, treats directly the problem of factorization of a modulus factorization of the module. In this Another version of GQ methods, proving context, "directly" means "without calling for the entity but also of the checking entity. here called elementary only

keys is defined by two necessary and sufficient conditions: n and the private number or numbers Q_I to Q_m are then at the number or numbers G_l to G_m . The factorization of the modulus number". square of a small number of numbers than I fixing a public exponent $v=2^k$ mechanism implements a parameter k, a small number greater level in the Each All the proving proving entity has its own modulus n. Each GQ2 $\{G_I,Q_I\}$ to $\{G_m,Q_m\}$. Each public number G_i is the key hierarchy. Each set of elementary g_i greater than 1 and called entities can use the , and one or several same public a "base

30

S

25

20

15

non-quadratic integers $= \pm g_i \pmod{n}$ does not have a solution in x in the ring of - for each base number, neither of the modulo n, that is to say that the numbers residues modulo n. two equations $\pm g_i$ are two

where $v=2^k$ has solutions in x in the ring of integers modulo private number Qi or its inverse modulo solutions. each base number, the equation $x^{\nu} \equiv g_i^2 \pmod{2}$ n is any one n.

10 15 S a result, many RSA models in use cannot establish a set of only half are congruent to 3 (mod 4) and half to 1 (mod modulus n must comprise at least two prime factors congruent elementary GQ2 keys. Thus, by taking high prime numbers at random, it appears that not allow a set of elementary GQ2 keys to be established, of which none or a single one is congruent to 3 (mod 4) does differs. Consequently, any modulus composed of prime factors which privileges the numbers ω (mod 4) relative to which the Legendre symbol $\pm g_i$ are two non-quadratic into account the second condition, the prime factors congruent residues modulo n, the to 3 (mod in order that of g_i $\mathbf{A}\mathbf{s}$

necessary with any technology overcome Here and sufficient principles. this limitation in order to be we introduce the sets of generalised GQ2 keys to RSA modulus whatsoever: with any modulus whatsoever, they depend and in particular able to use on two GQ2

20

GQ2 condition: The first principle reproduces the second elementary

25 $x^{\nu} \equiv g_i^2 \pmod{n}$ where $\nu = 2^k$ has solutions modulo n. For each base number g_I to in x in the ring of g_m , the equation

 q_i^2 - g_i^2 does not divide either trivial or not. When a number q_i is non different from the two numbers g_i and $n-g_i$, it is said that it is number the ring of integers modulo n. Depending on whether the transform it into a number a solution to the equation, number q thus reveals a breakdown of the modulus n. Because the private number Q or its inverse modulo n is q_i is equal to one of the two numbers g_i or n- g_i , or q_i which is a square successive squares q_{i} - g_{i} or q_{i} + g_{i} . Any non trivial trivial, n which divides k-1 modulo root of Gi in

30

$n = \operatorname{pgcd}(n, q_i - g_i) \times \operatorname{pgcd}(n, q_i + g_i)$

condition: The second principle widens the first elementary GQ2

- among the numbers q_1 to q_m , at least one number

S

10 15 set of generalised GQ2 keys which make it possible to use any integers modulo of generalised GQ2 keys are prime numbers modulus whatsoever, that is to say any composition of high Thus, the set of elementary GQ2 keys are certainly part of the the following cases: Each set of generalised GQ2 keys is in accordance least two of which are distinct. On the other hand, It is to be noted that if a number q+ exists while $\pm g_i$ are indifferently congruent to 3 or to 1 (mod 4) at n, the number two non-quadratic not sets of elementary q_i is manifestly non trivial residues in the with one of many GQ2

residues, this is a set of elementary GQ2 keys. when the 2xm numbers $\pm g_I$ to $\pm g_m$ are all non-quadratic

20 keys. keys, least one quadratic residue, this is not a set of elementary it is what is known here when among the 2xm numbers as a set of complementary $\pm gI$ to $\pm gm$, there GQ2 is at GQ2

25 preceding generalised GQ2 keys not being elementary. complementary principles, present GQ2 such a set must satisfy a third principle. invention keys, bу relates definition ō Besides the these the o f of

quadratic -among the 2xm numbers $\pm g_1$ to $\pm g_m$, there is at least one residue.

all analyse the breakdown of the modulus solution we provide, that is to say the invention, let us first of and trivial number "take next, In order to assess a square study the functions and then q, root" and then the notion of a quadratic the recall the "raise to the square" of rank in a Galois field CG(p); problem and understand the residue n revealed by a non Chinese in CG(p); and remainder in CG(p)

35

finally, analyse the applicability of the three principles stated

Analysis of the breakdowns of the module

roots in the ring; in other words, n divides Δ_i^2 -1. unit square roots. Each private number Q_1 to Q_m defines into f Galois fields $CG(p_I)$ to $CG(p_f)$. In each field, there are number unit square roots, that is ±1. In the ring, there are thus Just as p_1 to p_f , the ring of integers modulo n is broken down $\Delta_i = q_i/g_i \pmod{n}$ which is one of these 2^f unit square the modulus n is broken down into fprime

modulus n. $\Delta_{i}+1$ and therefore Δ_{i} does not reveal the breakdown • when q_i is trivial, that is to say $\Delta_i=\pm 1$, n divides Δ_i-1 , or of the

10

S

15 each field : the prime factor or factors dividing Δ_{i} -1 on the one $n=\operatorname{pgcd}(n, \Delta_{i}-1)\operatorname{xpgcd}(n, \Delta_{i}+1)$, resulting from the value of Δ_{i} in divide either Δ_{i-1} or Δ_{i+1} and thus Δ reveals a breakdown, this or these dividing when q_i is non trivial, that is to say $\Delta_i \Delta \pm 1$, n does not Δ_i +1 on the other.

the numbers q. Two numbers $\{q_1,q_2\}$ give a composite number Examination of the rules of multiplicative composition of

 $q_1 \times q_2 \pmod{n}$.

20

25

breakdown as q_I . when q_1 is non trivial and q_2 is trivial, the $q_1 \times q_2 \pmod{n}$ is non trivial; it reveals composite the same

composite number $q_1 \times q_2 \pmod{\frac{1}{2}}$ breakdown. when q_I and q_2 are n) is trivial; it does non trivial and $\Delta_1 =$ not reveal $\pm \Delta_2$ The

composite number $q_1 \times q_2 \pmod{n}$ is non trivial; it reveals breakdown. q_1 and q_2 are non trivial and $\Delta 1 \neq \pm \Delta 2$,

30

numbers, that is a total of 2^m-1 numbers. seven numbers; Three numbers $\{q_1,q_2,q_3\}$ give four composite q1xq3, q2xq3, m numbers thus $q l x q 2 x q 3 \pmod{n}$, that is provide 2^m-m-1 composite a total numbers

comprising i base numbers g_I to g_i and i private numbers Q_I to number q_{i+1} and thus a root Δ_{i+1} . another which are the unit roots. Let us try to take into account Q_i giving i numbers q_1 to q_i and therefore i numbers A_1 to A_i We shall now consider a set of generalised GQ2 keys base number g_{i+1} by a private number Q_{i+1} giving a

- trivial numbers in each of the following cases. • The total of the 2ⁱ⁺¹-1 numbers comprises as many non
- non trivial. the root Δ_{i+1} is trivial and at least one root Δ_1 to Δ_i is
- 2xi roots $\pm \Delta_1$ and $\pm \Delta_i$. The root Δ_{i+1} is non trivial and figures among the
- not figure among the 2xi roots $\pm \Delta_I$ to $\pm \Delta_i$, each composite • In the case where the root Δ_{i+1} is non trivial and does

15

10

Ŋ

number where q_{i+1} figures is non trivial.

Consequently, when among the m numbers q_1 to q_m , at numbers are non trivial. least one is non trivial, more than half the total of the 2^m-1

20 each of the 2^l-l-1 corresponding composite numbers is non $\{q_1,q_2,...q_l\}$ are independent relative to the modulus n when breakdown of the modulus n. trivial. Each of these 2^{I} -1 numbers thus reveals a different trivial, that is to say that, in total, the 2^{l} -1 numbers are all non By definition, it is said that l < f non trivial numbers

25 30 composite numbers. the f-1 independent numbers and the $2^{f \cdot l} - f$ corresponding independent, there is a bi-univocal correspondence between breakdowns $2^{f-I}-1$ breakdowns and a total of $2^{f-I}-1$ numbers comprising - When the f prime factors are distinct, there are $2^{f \cdot I}$ -1 of the modulus n. Thus, if f-l numbers q are

Chinese remainders

unique number and X_b from 0 to b-1; it concerns the determination of the themselves such as 0 < a < b, and two numbers X_a from 0 to a-1Either two numbers a and b, prime X from 0 to axb-1 such that $X_a \equiv X \pmod{a}$ and numbers between

operation is $X_b \equiv X \pmod{b}$. The number $x \equiv \{b \pmod{a}\}^{-1} \pmod{a}$ is remainders parameter. given below: The elementary Chinese the Chinese remainders

 $x \equiv X_b \pmod{a}$

Ŋ

 $y = X_a - x$; if y is negative, replace y by y + a

 $z \equiv \text{áxy (mod } a)$ $X = zxb + X_b$

To resume, one writes : $X = \text{Chinese Remainders } (X_a, X_b)$.

10 prime factors, that is to say f-1). parameters the smallest p_I to the biggest p_f , the Chinese remainder When f prime factors can be the following (there is one less than the are arranged in increasing order,

- The first parameter is $x \equiv (p_2 \pmod{p_I})^{-1} \pmod{p_I}$.
- The second parameter is $\beta \equiv (p_1 x p_2 (\text{mod} p_3))^{-1} (\text{mod} p_3)$.
- The *i*-th parameter is $\lambda \equiv (p_I \times ... p_{i-I} \pmod{p_i})^{-1} \pmod{p_i}$.
- And so on.

15

 X_f with X_j from 0 to p_{j-1} : from 0 to n-1 starting from any set of f components from X_I to In f-1 elementary operations, one establishes a number

- 20 a first result (mod $p_1 \times p_2$) with the first parameter,
- parameter, - then a second result (mod $p_1xp_2xp_3$) with the second
- parameter. - until the final result (mod $n = p_1 x p_2 x \dots p_f$) with the last
- 25 representations: the To resume, given the ring of integers prime factors p_I to p_f , each element modulo n has two equivalent
- $X_j \equiv X(\text{mod}p_j),$ f numbers X_{I} to X_f , a prime factor component:

30

35

sequence $\{X\}$ defined by $\{x_i = a; \text{ then, for } i \ge 1, x_{i+1} = a \times x_i \pmod{d} \}$ $(X_1,X_2,...X_f)$. definition, the rank of a with respect to p is the period of the number and a a number smaller than p i.e. Rank of numbers a number X from in CG(p) - Let p be an odd prime 0 to n-1, X=Chinese 0 ٨ remainders *a* <

 $a \times x_i \equiv x_{i+1} \pmod{p}$. Therefore, the rank of a number a with p)}. By applying the Fermat theorem we obtain: $x_{i+p} = a^p \times x_i = a^p \times x$ prime number p is p-1 or a divider of p-1.

all the non-zero elements of CG(p). sequence $\{X\}$ for indices from 1 to p'-1, form a permutation of successive powers of a generator in CG(p), i.e. the terms of the numbers of rank $2 \times p' = p-1$. In CG(p), any number of rank p-1number of rank 2: this is -1, p'-1 numbers the Galois field CG(p) includes a number of rank 1: this is 1, a "generator". For example, when (p-1)/2 is an odd prime number The name is due to the fact that of rank p' and p'-1

with p-1, this is p-1. When i divides p-1 this is (p-1)/i. In all the number $y' \pmod{y}$ according to i and divisor). cases, this Let y be a generator of CG(p). Let us evaluate the rank of is $(p-1)/\lg cd(p-1,i)$ ($\lg cd = \lg st common$ p-1. When i is prime

15

10

S

 $\varphi(p-1)$ generators. numbers smaller than n and prime with n. In CG(p), there definition, Euler's function $\varphi(n)$ is the number of

25 20 30 35 factors p-1 to p-f, with $f \ge 2$. For each prime factor facilitated with the rank. Module n is the product of f prime smallest common multiple (scm) of $(p_{1-}, p_{2-1}, \dots p_{f-1})$ divides permutation summarized by the public key $\langle e, n \rangle$. There exists expressed in the ring of integers modulo n by the RSA These f permutations, one in each field $CG(p_1)$ to $CG(p_f)$, are key $\langle d_j, p_j \rangle$ inverts the permutation of the elements of $CG(p_j)$. generally as small as possible, such that p_{-1} divides $e \times d_{j-1}$. The permutates the elements of $CG(p_j)$; there exists a number d_j , to p_f the public exponent e should be prime with p_{j-1} . Now, (mod p_{j-1}). The RSA permutation summarized by the public $d \times e$ -1. For each prime factor p_j from p_1 to p_f , we have $d_j \equiv d$ $\langle e, n \rangle$ is inverted by the private key $\langle d, n \rangle$. $\langle e, p_j \rangle$ As an illustration, understanding the bases of the RSA is d, generally as observes the rank of the elements of $CG(p_j)$: it small as possible, such that the p_i from p_I

p-1 is dividable by 2', but not by 2'-1. Each large congruent to 17 (mod 32), and so forth; on the average, one (mod 16), one out of sixteen in the fourth one, where p is one out of height in the third one, where p is congruent to 9 and so forth. If a sufficiently large number of successive prime appears in one and only one category: t = 1, t = 2, t = 3, t = 4, out of 2' appears in the nth category where p is congruent to first category where p is congruent to 3 (mod 4), one out of numbers are considered, $\pmod{2^{t+1}}.$ Squares second in CG(p) - Let us define a number t such that one, where p is congruent to 5 (mod 8), about one out of two appears prime number in the

0

S

15 "take orientated graph wherein each non-zero CG(p), key branches and cycles according to the parity of the rank of finds its place. Let us analyze the structure of the graph into the element. Because square" in CG(p)<2,p> numbers x and p-x have does not permutate may be element of the CG(p). The the same square represented by an function

20 related; the zero element is isolated. for The zero element is set. This is the zero element to which no other element is 0. Rank is not

25 30 th root of -1 referenced as b; indeed, we have $y^{(p-1)/2} \equiv -1 \pmod{p}$ branch related to 1. Let y be a non-quadratic residue of CG(p), of rank 1. All the roots 2^{t-1} , are the 2^{t-1} roots of unity other than 1: they make up Therefore, in CG(p), the branch related to 1. residue; key < p-1)/2', p> transforms y into a primitive 2'-The unit element is set. This is 1, the only element of unity in CG(p) are located in the powers of b for exponents from 1

element the rank of which is divided by two. Therefore, element ofa rank number The square of any element of even rank is another 2, two rank numbers rank is dividable placed in a branch; dividable by four but not by by two, but not by four each branch

sixteen but not by 32, and so forth. All the branches not by sixteen, next, if $t \ge 4$, eight rank numbers (p-1)/2' branches which are all of the same length t. elements and is related to an element of odd rank; there similar eight, next, if $t \ge 3$, four rank numbers dividable are non-quadratic to the branch related to 1; the 2'-1 leaves of each residues; each branch includes dividable by by eight but are

S

10 15 function $\varphi(p')$ is the number of numbers smaller than elements of rank p'. Let us recall that by definition, Euler's each divider number of cycles depends on the factorization of (p-1)/2'. For The permutation the unit element is another element having the same rank. Key the p'-1 numbers of rank p'prime with p'. For example, when p' equals (p-1)/2', is prime, <2,p> permutates The square of any element of odd rank other than p' of (p-1)/2', there is a cycle including the $\varphi(p')$ is factorized into permutation cycles. the set of (p-1)/2' elements of odd rank. form a large permutation cycle. p' and The

congruent to 32), respectively. Figures 1A-1D each illustrate a graph fragment for p 3 (mod 4), 5 (mod 8), 9 (mod 16) and 17 (mod

circles; these are non-quadratic residues. The leaves on the branches are illustrated by white The nodes in the branches are illustrated by grey

circles; these are these are The nodes in the cycles are illustrated as black circles; quadratic elements of even rank. quadratic elements of even rank.

25

20

equation x^2 residue of CG(p), let us see how to calculate a solution course, there Springer in Berlin Computation Algebraic Number Theory, published in 1993 Mathematics Square 31-36 $\equiv a \pmod{p}$ i.e. "take series (GTM 138), may be consulted. **roots** in CG(p) - Knowing that a is a quadratic are many ways for obtaining the same results; of the as volume 138 book of Henri Cohen, a Course a square root" ofthe Graduate in CG(p). Of to the

which is: The number $s = (p-1+2^t)/2^{t+1} \text{ provides}$ a key $\langle s, p \rangle$)

<(p+7)/16, p> when p is congruent to 9 <(p+3)/8, p><(p+15)/32, p> when p is congruent to 17 (mod32), <(p+1)/4, p> when p is congruent to 3 (mod4), when p is congruent to 5 (mod8), (mod16),

S

and so forth.

10 the solution of odd rank, we name it w. Indeed, in CG(p), w^2/a The other solution is of even rank; this is p-w. is equal to the previous element in the cycle. When a is of even rank, a to the power of $(2\times (p-1+2^t)/(2^{t+1})-1) = (p-1)/(2^t)$ Key $\langle s, p \rangle$ transforms any element of a cycle into it is

20 15 name r. As a is a quadratic residue, to any primitive 2^t th root of 1 in the field CG(p). Therefore, residue a in a first approximation, into a solution the key $<2^{t-2}$, p> transforms the new approximation into 1. It The new approximation remains r if the result is +1 or else it take the power 2^{t-2} of $r^2/a \pmod{p}$ in order to obtain +1 or -1. transforms r^2/a into 1. To approach a square root of a, let us may still be approached by using the key $<2^{t-3}$ becomes $b \times r \pmod{p}$ if the result is -1, knowing that p refers multiplying with $b2 \pmod{p}$ if necessary, and so forth. Generally, the key $\langle s, p \rangle$ transforms any quadratic the key $<2^{t-1}$, p> certainly $^{\circ}$, p and by which

25 numbers a, b, p, r and t, as defined above and two variables: cp-w= r. At the end of the calculation, the two solutions approximations. The following algorithm solves the equation. the successive corrections and w the At the beginning of the algorithm, c = b and wsuccessive are

For i from t-2 to 1, repeat the following sequence:

- obtain +1 or -1. - Apply key <2', p> to number $w^3/a \pmod{mod}$ p) in order t o
- When -1 is obtained, replace w by $w \times c \pmod{p}$.
- Replace c by $c2 \pmod{p}$.

state that a parameter k, a base number g and a prime factor p are *compatible* when the equation $x^{\vee} \equiv g^2 \pmod{p}$ where exponent v is 2^k , has solutions in x in the field CG(p). Numbers number. g are small and larger than 1. Number p is a large prime Applicability of the principles **■** 82 By definition

S

solutions. - When t = 1, i.e. $p \equiv 3 \pmod{4}$, the equation has two

10 solutions if $(g \mid p) = +1$; it does not have any solution if $(g \mid p) =$ Legendre symbol of g with respect to p, the When t | 2, i.e. p =Ŋ (mod 8), equation has four according to

15 respect to p, but such that 2^{u+1} does not divide it; therefore, uis equal to one of the numbers from 0 to t-1. The equation has that 2" divides the rank of the it has 2' solutions if u = 0 and k > t. no solution if u > 0 and k + u > t; it has 2^k solutions if $k + u \le t$; - When t > 2, i.e. $p \equiv 1 \pmod{8}$, let u be the number public number G =82 such

20 to whether G is in a cycle, or else in a suitable position in a branch. Therefore, there are two types of compatibility according

consecutive branches related to the cycle, i.e. 2^{α} solutions value of k, there is a solution of odd rank in the cycle all. Figure 2A illustrates this case with $k \ge t = 3$, i.e. a prime solutions of even rank disseminated in $\alpha =$ When G is in a cycle, i.e. u = 0, regardless of the $\min(k,$ and

25

30

factor congruent to 9 (mod 16), which imposes that u = 0. branch. Figure $u+k \leq t$, there When G is in a suitable position in a branch, i.e. u > 0 and 2B illustrates this case. are 2^k solutions, all of even rank and in the

prime factors or else larger than or equal to k. according to whether the value of t is less than kparameter k, there are therefore two types

should be in a cycle, and there For any prime factor p_j , such as tis no solution in the ٨ k, each branch

 p_j congruent to 9 (mod 16), i.e. u = 0, t = 3 with k > 3. according to whether g_i or $-g_i$ is in the cycle. There is illustrates a case with t < k: G_i is in a cycle with a prime factor choice for any of the *m* numbers $\Delta_{I,j}$ to $\Delta_{m,j}$. Figure 3A related to G_i . Let us define a number $\Delta_{i,j}$ which is +1 n o

S

10 us define a number $\Delta_{i,j}$ which is +1 or -1 according to whether should be such that $u + k \le t$, i.e., either in a cycle with u = 0 Q_{ij} is in the portion of the graph related to g_i or to $-g_i$. There is or else, in a suitable position in a branch with $1 \le u \le t-k$. Let may individually be switched from one value to the a choice for each of the m numbers $\Delta_{I,j}$ to $\Delta_{m,j}$; each number $\Delta_{i,j}$ with k = 3. prime factor p_j congruent to 17 (mod 32), i.e., u = 1, t = 1**Figure** 3B illustrates a case when $t \ge k$: G_i is in a branch with a For any prime factor p_j such that $t \ge$ k, each G_i other.

of f components is constant or variable, which expresses the the f components are equal or not; we then state that the set components $Q_{i,j}$. summarizes a number q_i is non-trivial, the set of f components $\{\Delta_{i,l}...\Delta_{i,f}\}$ fact that the number q_i is either trivial or not. Therefore, when unity in $CG(p_j)$. This root is trivial or not according to whether possible to test the principles before calculating the private Each set of f components $\{\Delta_{i,I}...\Delta_{i,f}\}$ is a square a factorization of the module. It is therefore root of

20

15

25 symbol: $\Delta_{i,j} = (g_i | p_j)$. $-g_i$ is in the cycle. When $p_j \equiv 3 \pmod{4}$, this is Legendre's factor p_j , the number $\Delta_{i,j}$ is +1 or -1, according to whether g_i or When a public number G_i is in a cycle for a prime

30 a branch for a prime factor p_j , the value to be given to $\Delta_{i,j}$ may be determined by computing the private component Qi,. When a public number Gi is in a suitable position in

there are Production of sets of keys - Given a parameter two strategies. k,

order to determine m base numbers. The first prime numbers: Either the generator requires f prime factors

number may thereby be obtained by composing the numbers cycle, exactly as a square brings the cycle closer. in a similar position in a branch, their product is closer to the with each of the f large prime factors p_1 to p_f . Although g = 2 is which are not appropriate individually. composition of a base number. Indeed, when two numbers are not compatible with $p \equiv 5 \pmod{8}$, 2 may enter into the 2, 3, 5, 7, ... are examined for evaluating their compatibility A base

S

15 10 numbers: 2, 3, 5, 7, 11 ... or else these are combinations of the characteristics of the module such that a bit size (for example, the size assigned to the module divided by f. n will be the product of f prime factors with close sizes, i.e. note that $p \equiv 5 \pmod{8}$, is not compatible with g = 2. Module first prime numbers. Unless indicated otherwise, these are the the base numbers order to determine $f \ge 2$ prime factors. Noted as G_I , G_2 ,... G_m , to 1 with strong weights (for example, 1, 8, 16, 24, 32) in 512, 768, 1024, 1536, 2048) and a number of bits successive first m prime numbers; $G_1 = 2$, $G_2 = 3$, $G_3 = 5$, $G_4 = 7$,... Let us Or the generator requires m base numbers generally appear among the first prime and

25 rank of g with respect to p, whereas 2^{h+1} does not divide it. To of unity in CG(p). compatible. Let us define a number h such as 2^h divides from p_I to p_f and each base number g from g_I to g_m should be Legendre's compute First principle the number h, the following procedure symbol (g | p) and a number b, a primitive - The parameter k, each prime factor 2'th root

If $(g \mid p) = +1$ with t = 1, return "h = 0". If $(g \mid p) = +1$ with t > 1, apply the key $(p-1+2^t)/2^{t+1}$, p

> to G in order to obtain a result called w. If w = +g, return "h = 0".

30

If w = p-g, return "h = 1".

Else, set c to b and for i from t-1 to 2,

Apply key $\langle 2^i, p \rangle$ to $w/g \pmod{p}$ in order to obtain

- If -1, set h to i and replace w with $w \times c \pmod{p}$,
- Replace c with $c2 \pmod{p}$.
- Return "value of h from 2 to t-1"
- If (g | p) = -1, return "h = t".

S

of the value of k, and equally when k > 1 with $k+h \le t+1$. with k+u>t; they are compatible when h=0 or 1, regardless Let us recall that k, g and p are incompatible when u > 0

15 10 correspond to different implementations of certain aspects of the demonstration q_1 to q_m be not trivial. The role of the base numbers may be reinforced to the point of requiring that each number principle. In certain implementations, balanced; balancing or not the second principle has an effect among the *m* numbers $\{q_1 \dots q_m\}$, it may be required that there at least one subset of f-1 independent numbers. Second principle -Finally, when there are f > 2The three distinct prime factors, the second principle following procedures of the security of the \mathbf{of} the is then

The three procedures use $m \times f$ numbers $\delta_{i,j}$ defined as

follows.

20 $\Delta_{i,j}$, i.e. +1 if $h_{i,j} = 0$ and -1 if $h_{i,j} = 1$. When p_j is such that t < k, for i from 1 to m, $\delta_{i,j} =$

which means that $\Delta_{I,j}$ to $\Delta_{m,j}$ may be selected according principle. When p_j is such that $t \ge k$, for i from 1 to m, $\delta_{i,j} = 0$, to the

non-trivial or may be chosen as non-trivial. is variable or zero, i.e. that at least one number A first procedure ascertains that at least one set $\{\delta_{i,I} \dots$ q_I to q_m is

25

For i from 1 to m and j from 1 to f,

if $\delta_{i,j} = 0$ or $\neq \delta_{i,I}$, return "success".

- Return "failure".

30

or may be variable or zero, i.e. that each number q_I to q_m is non-trivial A second procedure ascertains that each set $\{\delta_{i,l} \dots \delta_{i,f}\}$ is chosen as non-trivial.

For i from 1 to m,

- For j from 1 to f,

- if $\delta_{i,j} = 0$ or $\neq \delta_{i,l}$, skip to the next

Return "failure"

Return "success".

Ŋ when m is smaller than f-1. When it succeeds, $\delta_{i,f}$ where $\delta_{i,jl}$ is zero or different from $\delta_{i,j2}$. It obviously fails p_{jl} and p_{j2} , with $1 \le j_1 \le j_2 \le f$, there is at least one set $\{\delta_{i,l} \dots$ numbers A third_procedure_ ascertains that each pair of prime factors q_I to q_m , there is at least one set of independent f-1 among

numbers with respect to the f prime For j_1 from 1 to f-1 and for j_2 from j_1 +1 to f, factors.

10

For i from 1 to m,

- If $\delta_{i,jl} = 0$ or $\neq \delta_{i,j2}$, skip to the next values of j_1 and j_2 ,

Return "failure".

Return "success".

15

follows its strategy chosen from the two possible strategies: When a procedure fails, the generator of GQ2 key sets

the f prime Change one of the m base numbers while keeping factors,

m base numbers. Change one of the f prime factors while keeping the

20

production or already produced, is whether the set of Third principle - The following procedure either a set of elementary GQ2 keys, i.e. that the generalized GQ2 keys, either during determines

 $2 \times m$ numbers $\pm g_I$ to $\pm g_m$ are all non-quadratic residues,

25

quadratic among the $2\times m$ numbers $\pm g_I$ to $\pm g_m$, there is at least or else, a set of complementary GQ2 keys, i.e. that

30 $(-g_i | p_j)$ for i from 1 to m and for j from 1 to f. The procedure uses both Legendre's symbols $(g_i | p_j)$ and

For i from 1 to m,

For j from 1 to f,

If $(g_i | p_j) = -1$, skip to the next value of i.

Return "set of complementary GQ2 keys"

For j from 1 to f,

If $(g_i | p_j) = -1$, skip to the next value of i.

Return "set of complementary GK2 keys"

Return "set of elementary GK2 keys"

S

followed by the more complex case, i.e. t > 2. simplest and most current cases, i.e. t = $\equiv g_i^2 \pmod{p_j}$ the following computation establishes all the Private components - For an equation of the direct type: values for the private component $Q_{i,j}$. The two 1 and t = 2, are

provides the quadratic square root of any quadratic residue in For t = 1, i.e. $p_j \equiv 3 \pmod{4}$, the key $<(p_j+1)/4, p_j>$

 $CG(p_j)$. From this, a number is derived

or p_j -w. transforming G_i into $w \equiv G_i^{sj} \pmod{p_j}$. $Q_{i,j}$ is equal to w $\equiv ((p_j+1)/4)^k$ (mod $(p_j-1)/2$), which gives a key

15

10

20 (mod $(p_j-1)/4$), which gives a key $\langle s_j, p_j \rangle$ transforming G_i into $w \equiv G_i^{(y)}$ (mod p_j). Let us note that $z \equiv 2^{(p_j-1)/4}$ (mode p_j) is a p_j) or p_j -w'. $(p_j).$ $Q_{i,j}$ is either equal to w or to p_{j} -w or else to $w' \equiv w \times z$ (mod square root of -1 because 2 is a non-quadratic residue in CG rank in $CG(p_j)$. From this, a number is derived $s_j = ((p_j+3)/8)^k$ provides the square root of odd rank for any element of odd For t = 2, i.e. $p_j = 5 \pmod{8}$, the key $<(p_j+3)/8, p_j>$ (mode p_j) is a

25 For $p_j \equiv 2^t+1 \pmod{2^{t+1}}$ with t > 2, key $<(p_{j^-}1+2^t)/2^{t+1}$, $p_j>$ provides the square roo and p gave the value of h, next that of u. any element of odd rank. The compatibility test between k, g, pj> provides the square root of odd rank of

of k), a number is established, When G_i is in a cycle (u = 0, regardless of the value

30 roots of unity in $CG(p_j)$. transforms G_i into the solution of odd rank $w \equiv G_i^{sj} \pmod{p_j}$. consecutive branches. $Q_{i,j}$ is equal to the product of w by any of the $s_j \equiv ((p_{j-1}+2')/2'^{+l})^k \pmod{(p_{j-1})/2^t}.$ solutions of even rank distributed in min(k, t)branches related to the cycle, let us Key say, in α

 $k \le t$), all the solutions are in the same branch as G_j , a branch number is established as related to a cycle by the 2"th power of the number G_i . A When G_j is in a suitable position in a branch (u > 0, u +

 $s_j \equiv ((p_{j-1}+2^t)/2^{t+1})^{k+u} \pmod{(p_{j-1})/2^t}$

S

number of odd rank w. The set of products of w with the values of $Q_{i,j}$. primitive 2^{k+n} th roots of unity in $CG(p_j)$ comprises the 2^k Key $\langle s_j, p_j \rangle$ transforms the 2^uth power of G_i into a

10 unity. may be switched by multiplying $Q_{i,j}$ by a primitive 2^k th root of root is a primitive 2^k th root of unity. The value of number $\Delta_{i,j}$ of unity in $CG(p_j)$, the 2^{t-u} th power of b_j in $CG(p_j)$ exists; When p_j is such that $t \ge k$, as number b_j is a primitive

15 congruent to 5 (mod 8) $\langle s_j, p_j \rangle$, which amounts to inverting the value of $Q_{i,j}$ in $CG(p_j)$. is sufficient to replace number s_j with $((p_{j-1})/2^t)-s_j$ in the key For an equation of the inverse type: $1 \equiv x^{\nu} \times g_i^2 \pmod{p_j}$, it of a set of keys with two prime factors

20 4C435C95F32BF25 E6C83BF428689AF8C35E07EDD06F9B39A659829A58B79CD89

25 11BF8A68A0817BFCC00F15731C8B70CEF9204A34133A0DEF8

D5F42C0126F5BD6B05478BE0A80ED1 B650E9AB9AAD2EB713CD4F9A97C4DBDA3828A3954F296458 FFFF8263434F173D0F2E76B32D904F56F4A5A6A50008C43D32 62829B2EEA74873D $p_1 \times p_2$

30 numbers. Here are the Legendre symbols of the very first prime

$$(2 \mid p_I) = -1;$$
 $(3 \mid p_I) = -1;$ $(5 \mid p_I) = +1;$ $(7 \mid p_I) = -1;$ $(11 \mid p_I) = +1;$ $(13 \mid p_I) = -1;$ $(17 \mid p_I) = +1;$

In $CG(p_I)$, the rank is odd for -5, -11 and 17

35
$$(2 | p_2) = -1; (3 | p_2) = +1; (5 | p_2) = +1; (7 | p_2) = +1;$$

 $(11 | p_2) = +1; (13 | p_2) = -1; (17 | p_2) = -1;$ In CG(p_2), the rank is odd for 3, -5, 7 and 11.

Carmichael's function is $\lambda(n) = \text{scm}((p_1-1)/4, (p_2-1)/4).$

Ŋ

5A1B37239B18FA9B0F618627D8C7E1D8499C1B 3334F40C3D57A9C8558555D5BDAA2EF6AED17B9E3794F51A6 $\lambda(n)=33331A13DA4304A5CFD617BD6F83431164212154$

generic equations of the inverse type. $(\text{mod }\lambda(n))$ is used as a private With k = 9, the number σ exponent, in order to use the $\lambda(n) - ((1+\lambda(n))/2)^9$

10

= 01E66577BC997CAC273671E187A35EFD25373ABC9FE6770E 2416D4CC 1121E7A7A8B6AE186BB4B0 7446C0CCEF2C72AF6E89D0BE277CC6165F1007187AC58028BD

15 numbers. Numbers 2, 3, 7, 13 and 17 are not suitable as base

-5 is on a cycle. which does not shows any factorization. Indeed, in both fields, Key $\langle \sigma, n \rangle$ transforms 81 = 5 into a private number 0

20 0 4BD47C5D6E0E7EBF6D89FE3DC5176C 818C23AF3DE333FAECE88A71C4591A70553F91D6C0DD5538E C0F2AAF909B5BDAD491FD8BF13F18E3DA3774CCE19D0097BC

25 position in both fields. which shows Key $\langle \sigma, n \rangle$ transforms $g_2 = 11$ into a private number a factorization. Indeed, 11 is not in the same

50DA052089EEC96A1B7DEB92CCA7 5196B07C19080DC962E4E86ACF40D01FDC454F2565454F2900 25F9AFDF177993BE8652CE6E2C728AF31B6D66154D3935AC53

number Q_3 which shows a factorization. 167D99532B3A96B6BF9D93CAF8D4F6AF0 67D18A0459A1254121E95D5CAD8A1FE3ECFE0685C96CC7EE86 $Q_3 = 78A8A2F30FEB4A5233BC05541AF7B684C2406415EA1DD$ Key $\langle \sigma, n \rangle$ transforms $g_3 = 21 =$ 3×7 into a private

35

S

number Q_4 which shows a factorization. $\langle \sigma, n \rangle$ transforms 8 | 26 2×13 into þ private

481B738C62BF8C673731514D1978AF5655FE493D659514A6CE 6F1748A6280A200C38824CA34C939F97DD2941DAD300030E 897AB76C01E50B5488C5DAD12332E5

Ø

eight prime private The private key may further be represented factors, the parameter of the Chinese remainders components. both and

10 ADE4E77B703F5FDEAC5B9AAE825D $(p_2 \pmod$ $(p_I)^{-1} \pmod{p_I}$

||

649E06692D15FBF0DF737B115DC4D012FD1D $Q_{I,I} \equiv Q_I(\text{mod } p_I) =$

15 9AF4D229949C74DD6C18D76FAF $Q_{1,2} \equiv Q_1 \pmod{p_2} =$

7751AEE918A8F5CE44AD73D613A4F465E06C6F

5FD48152C08EEB6114F31B7665F A9EB5FA1B2A981AA64CF88C382923DB64376F

 $Q_{2,I} \equiv Q_2(\bmod p_I) =$

20 4004ABB2C2AC1CA3F5320C5A9049 D5A7D33C5FB75A033F2F0E8B20274B957FA3

76C9F5EFD066C73A2B5CE9758DB512DFC011 $Q_2 \pmod{p_2}$

F5B5AF7DA8D39A961CC876F2DD8F

25 2FEC0DC2DCA5BA7290B27BC8CC85C938A514 $Q_{\beta,I} \equiv Q_3(\bmod p_I) =$

B8F5CFD55820A174FB5E6DF7B883

 $Q_{3,2} \equiv Q_3 \pmod{p_2} = 010D488E6B0A38A1CC406CEE0D55DE59$

013389D8549DE493413F34604A160C1369

30 4652145EE159DF3DC0C61FE3617 A2B32026B6F82B6959566FADD9517DB8ED852 $Q_{4,I} \equiv Q_4(\bmod p_I) =$

 $Q_{4,2} \equiv Q_4 (\bmod p_2) =$

011A3BB9B607F0BD71BBE25F52B305C22489

9E5F1F8CDC2FE0D8F9FF62B3C9860F

consists in storing m private numbers Q_i and the public main representations which are possible for the GQ2 private entity but not within the controlling entity. on the progress of the computations key. The representation of the GQ2 private key has an effect prove to be equivalent: they all amount to knowing components parameter k, representation in terms of work loads consists is in competition with the following two. 2) checking key $\langle v, n \rangle$; for the GQ2 schemes, this representation key. 1) The conventional representation of GQ private keys factorization of the module n which is the actual GK2 private remainders so that it amounts to the second representation. private components $Q_{i,j}$ and the f-1 parameters of the Chinese module n so that it amounts to the first representation, or $m \times f$ numbers g_i and the f prime factors p_j , and then in starting each private key size consists in storing the parameter k, the m base remainders. use by establishing either m private numbers Polymorphism possible representations 3) $Q_{i,j}$ and the f-1 parameters of the fThe optimum representation of the private prime factors p_j , the of the within the demonstrating key Here are the three private key The optimum in storing Q_i and the $m \times f$ in terms the Chinese private GQ2 the

mechanism or of the digital signature is equivalent to knowing specified, two of which are known to an entity and the other simply. Generally, each proving entity has its own GQ2 a factorization of the module, with the GQ2 schemes, two to another one. However, GQ2 modules with four prime factors possible to distinguish two entities using the same Because the security of the dynamic authentication may module. it is not module bе

25

30

Ċ

20

15

10

S

associated controller, the authenticity of another entity authentication mechanism is for proving to an entity demonstrator as Dynamic message M, so that the controller ascertains authentication well as the authenticity The of ы called dynamic possible called a that it

itself and the demonstrator are speaking of the same is actually dealing with the demonstrator M. The associated message M is optional, which means it may and optionally that message

S checking acts. and and four response a checking The dynamic authentication mechanism is a sequence an engagement act, a challenge acts. act. The controller plays The demonstrator plays the engagement act, the challenge a response and

15 10 according and the GQ2 private key, i.e. the factorization of the module nisolated, in order commitments numbers and the module n. parameters functions Within • the f prime factors components, to one of the Chinese remainders, • the m private and responses. the of the demonstrator, i.e. the production of the to isolate demonstrator, the f prime and the m base numbers, three representations The witness has the parameter kthe most sensitive factors 90 witness and parameters mentioned may • the $m \times f$ the

20 25 chip card. The thereby isolated witness is similar to the witness many challenges d. Each set $\{R, d, D\}$ forms a GQ2 triplet. execution of the mechanism, the witness produces one or defined hereafter within a PC or even • programs particularly protected within a example • a chip card connected to a PC forming together demonstrator or commitments witness may correspond to a particular embodiment, within the signing R, and then as many responses D to even • programs particularly entity. Upon each protected as

demonstrator also has a hashing function necessary. addition to it comprising and a message the witness, the

30

keys; if necessary, it also has the same hashing function and a message M'. The GQ2 public parameters, i.e. numbers k, m and directory The controller has of public keys or even from the module n, for example, from a a certificate of public

20 10 15 Ŋ challenges referenced commitment R' from any challenge prime numbers. Each challenge d should include m elementary otherwise, the m base numbers demonstrator. security, triplets may be produced in parallel; they may also be chance of success quartets. bits). For example, with k = 5 and m = 4 base numbers, 5, 2^{k-1} -1 (numbers from v/2 to v-1 are not used). Typically, each mechanism. produced dynamic brought by each GQ2 triplet: an impostor who by definition, probable, 21 and 26, each challenge includes 16 bits transmitted Parameters k and m inform the controller. Unless indicated not know the elementary to 20, one triplet is sufficient for reasonably in sequence, authentication. is coded by m times k-1 bits the When the possible may The number $(k-1)\times m$ determines challenge from d_I to d_m is a number from 0 to be out of $2^{(k-1)\times m}$ factorization of the module from d_1 to d_m : one provided i.e. repeat In order to achieve any level $(k-1)\times m$ challenges from g_1 to g_m are the first mis Ç ', exactly. When $(k-1)\times m$ is d and from any the the execution (and controller per base not m times kthe security n, has are number ensuring on four equally of the o f

operations. The act of commitment comprises the following

25

30 number r into a squaring random the parameter k, the m private numbers from Q_1 to Q_m and When the witness does not use the Chinese remainders, n; it randomly and privately numbers r (0 them k times (mod n), it transforms each random commitment R. $R \equiv r^{\vee}$ < r < n); and then by successively picks one or

(mod n)

Chinese remainders an example with the previous set of keys without

5E94B894AC24AF843131F437C1B1797EF562CFA53AB8AD426C

8F09C60D981512198126091996 1AC016F1C89CFDA13120719477C3E2FB4B4566088E10EF9C010E

S

6D7068D083EF7C93F6FDDF673A 00EBF234FA0BC20A95152A8FB73DE81FAEE5BF4FD3EB7F5EE3E3 6BBF9FFA5D509778D0F93AE074D36A07D95FFC38F70C8D7E33

random number r_i into a commitment component R_i . successively squaring it k times (mod p_i), it transforms random number r_i per prime factor p_i (0 < r_i < p_i); and then by collections of f random parameter components parameters When the witness uses the Chinese remainders, it has the k, the first f prime $Q_{i,j}$; it randomly and privately picks of Chinese numbers: every collection includes one remainders factors from p_1 to p_f , f-1 and $m \times f$ private one or more

10

15

remainder witness establishes a commitment according $R_i \equiv r_i{}^V \pmod{p_i}$ For each collection of f commitment components, are random number collections technique. There are as many commitments to the Chinese the

Chinese remainders $(R_1, R_2, \dots R_f)$

20

Chinese remainders. Here is an example with the previous set of keys and with

 $\mathbf{r}_1 =$ 44FDF0204E84D8CAE 5C6D37F0E97083C8D120719475E080BBBF9F7392F11F3E2

25 4DD4FE20C5C7C5E205DF66 $R_1 = 3DDF516EE3945CB86D20D9C49E0DA4D42281D07A7607$

ED15DBFCB9A4915AC3 AC8F85034AC78112071947C457225E908E83A2621B0154

 $R_2 = 01168CEC0F661EAA15157C2C287C6A5B34EE28F8EB4D8D$

30 340858079BCAE4ECB016

 $R = Chinese remainders (R_1, R_2) =$

0AE51D90CB4FDC3DC757C56E063C9ED86BE153B71FC65F47C1 23C27F082BC3DD15273D4A923804718573F2F05E991487D17 DAE0AAB7DF0D0FFA23E0FE59F95F0

controller, either all or part of each hashing code H obtained by hashing each commitment R and a both cases, the demonstrator commitment transmits R, or else the

challenges $d_1, d_2, \dots d_m$; each elementary challenge the numbers from 0 to v/2-1. d =or more challenges d, each consisting 2) **The** act of challenge consists in randomly picking of m d_i is one of elementary

S

10 $d_I =$ and $d_1 d_2 \cdots d_m$ $1011 = 11 = 'B'; d_2 = 0011 =$ Here is a challenge for both examples, 4 3; $d_3 = 0110$ i.e. 6; with 11 1001K S

d = $d_1 \parallel d_2 \parallel d_3 \parallel d_4 =$ 1011001101101001 =В3

demonstrator. The controller transmits each challenge Ω o the

15

operations. 3) The act of response includes the following

20 numbers according to the elementary challenges. random number r from the commitment act and the private module parameter k, the m private When the witness does not use Chinese remainders, it has n; it computes one or more responses numbers from Q_1 to Q_m and the D by using each

 $D \equiv r_i \times Q_i^{d1} \times Q_2^{d2} \times \dots Q_m^{dm} \pmod{p_i}$

Chinese remainders. Here is the continuation of the example without the

25

027E6E808425BF2B401FD00B15B642B1A8453BE8070D86C0A7 BA648FD8E86BE0B2ABCC3CCBBBE4 870E6C1940F7A6996C2D871EBE611812532AC5875E0E116CC8

computes parameter remainder using When the witness uses one each k, f prime parameters or more collection factors from p_1 to and $m \times f$ private collections of random Chinese remainders, of f response components numbers p_f , the f-1 components it has the from Chinese $Q_{i,j}$; it

35

includes one commitment component per prime factor. act: each collection of response components

$$D \equiv r_i \times Q_{1,i}^{d1} \times Q_{2,i}^{d2} \times \dots Q_{m,i}^{dm} \pmod{p_i}$$

establishes For each collection of response a response There are as many responses according to the Chinese components, as

S

remainders. $D = \text{Chinese remainders}(D_1, D_2, \dots D_f)$ Here is the continuation of the example without the Chinese

10

$$D1 = r_i \times Q_{1,1}^{d_1} \times Q_{2,1}^{d_2} \times Q_{3,1}^{d_3} \times Q_{4,1}^{d_4} \pmod{p_{\ell}}$$

$$C71F86F6FD8F955E2EE434BFA7706E38E5E715375BC2CD2029A$$

 $D2 = r_2 \times Q_{1,2}^{d1} \times Q_{2,2}^{d2} \times Q_{3,2}^{d3} \times Q_{4,2}^{d4} \pmod{p_2}$

15 0BE022F4A20523F98E9F5DBEC0E10887902F3AA48C864A6C354 693AD0B59D85E

9073B9418CA5EBF5191218D3FDB3 8577A660B9CFCEAECB93BE1BCC356811BF12DD667E2270134C 90CE7EA43CB8EA89ABDD0C814FB72ADE74F02FE6F098ABB98C

20

D to the controller. In both cases, the demonstrator transmits each response

triplet $\{R, d, D\}$ satisfies an equation of the following type for a 4) The act of checking consists in checking that each

$$R \times \prod_{i=1}^{m} G_i^{d_i} \equiv D^{2^k} \pmod{n} \text{ or else } R \equiv D^{2^k} \times \prod_{i=1}^{m} G_i^{d_i} \pmod{n}$$

or, in restoring each commitment: none of them must be

$$R' \equiv D^{2^k} / \prod_{i=1}^m G_i^{d_i} \pmod{n}$$
 or else $R' \equiv D^{2^k} \times \prod_{i=1}^m G_i^{d_i} \pmod{n}$

hashing code H. commitment act, i.e., all or part of each commitment R, or the M'. Dynamic authentication is successful when the controller H' by hashing Optionally, the controller then computes a hashing code each restored commitment R' and the message what it has received at the end of

S

10 15 challenge d_I , indicates square and the i+1-th square, the i-th bit of the elementary division or multiplication, which is performed between the i-th multiplications (mode n) by base numbers. For the i-th comprises k squares (mod n) separated by k-1 divisions or transforms response the i-th bit of the elementary d_m which indicates if g_m must elementary example, challenge d_2 indicates а D into a commitment R'. The sequence if g_1 must be used, the i-th bit of the sequence of elementary operations if g_2 must be used, ... up to

remainders. Here 1sthe end of the example without the Chinese

20 027E6E808425BF2B401FD00B15B642B1A8453BE8070D86C0A7 Take the square modulo n: BA648FD8E86BE0B2ABCC3CCBBBE4 870E6C1940F7A6996C2D871EBE611812532AC5875E0E116CC8

25 88BA681DD641D37D7A7D9818D0DBEA82174073997C6C32F7 376CAF5DCE B644F098FAF3B1EB49B39 FCAB30380C4C6229B0706D1AF6EBD84617771C31B4243C2F0

30 A840FDE008B415028AB3520A6AD49D CAAD7AFE192B9440C1113CB8DBC45619595D263C1067D3D0 6ECABA65A91C22431C413E4EC7C7B39FDE14C9782C94FD6FA3 Multiply by 5 times 26 = 130, i.e. '82' modulo n:

D64CF75C4F652031041328B29EBF0829D54E3BD17DAD21817 0236D25049A5217B13818B39AFB009E4D7D52B17486EBF844 4A01E6E3AA650C6FD62CC274426607 the square modulo n:

4504A92834BA405559256A705ABAB6E7F6AE82F4F33BF9E912 2E7F40960A8BBF1899A06BBB6970CFC5B47C88E8F115B5DA59 Multiply 27F0ACFA4A052C91ABF389725E93 modulo

569B53D42DAD49C956D8572E1285B0 B802171179648AD687E672D3A32640E2493BA2E82D5DC87D Take the square BA2B2CC0325E7A71C50E8AE02E299EF868DD3FB916EBCBC0C5 modulo n:

modulo n: Multiply by 5 times 11 times 21 1155, '483

10

S

3305560276310DEFEC1337EB5BB5810336FDB28E91B350D485 248A8DC417C667B419D27CB11F72 B09188E0C4F1D67E68E9590DB7F9F39C22BDB4533013625011 Take the square modulo n:

15 8871C494081ABD1AEB8656C38B9BAAB57DBA72A4BD4EF902 9ECBFFF540E55138C9F22923963151FD0753145DF70CE22E9D0 19990E41DB6104005EEB7B1170559

modulo Multiply by 5 times 11 times 26 1430, i.e. 1596

20 7045ECFFF88F5136C7FBC825BC50C 2CF5F76EEBF128A0701B56F837FF68F81A6A5D175D0AD67A14 DAEC6FB68C362B1DC0ADD6CFC004FF5EEACDF794563BB09A1

25 6BBF9FFA5D509778D0F93AE074D36A07D95FFC38F70C8D7E33 6D7068D083EF7C93F6FDDF673A 00EBF234FA0BC20A95152A8FB73DE81FAEE5BF4FD3EB7F5EE3E3 the square modulo

successful. The commitment 7 1Sretrieved. Authentication

remainders Here 1sthe end ofthe example with the Chinese

30

90CE7EA43CB8EA89ABDD0C814FB72ADE74F02FE6F098ABB98C 9073B9418CA5EBF5191218D3FDB3 8577A660B9CFCEAECB93BE1BCC356811BF12DD667E2270134C

Take the square modulo n:

33B136EBE3EB5F13B170DD41F4ABE14736ADD3A70DFA43121 770192532E9CED554A8690B88F16D013010C903172B266C11 B6FC5560CDD4B4845395763C792A68

Multiply by 5 times 26 = 130, i.e. '82' modulo *n*:

S

90AE3646B461D3521420E240FD4 6EE9BEF9E52713004971ABB9FBC31145318E2A703C8A2FB3E144 E7786397CD8D1910E70FA86262DB771AD1565303AD6E4CC6E

Take the square modulo n:

10 9E664C23CA0E04E84F2F0AD65340 60B2126CBBDFC734E39F2C9A39983A426486BC477F20ED2CA5 D9840D9A8E80002C4D0329FF97D7ADl63D8FA98F6AF8FE2B21

Multiply by 21, i.e. '15' modulo n:

0C7782B5941924BB4BE91F86BD85F D7DD7516383F78944F2C90116E1BEE0CCDC8D7CEC5D7D1795 ED33BFE8623DB3D2E5B6C5F62A56A2DF4845A94F32BF3CAC36

Take the square modulo n:

15

B914855310C75BCA328A4B2643DCCDF 021B626ADAFBAB5C3F1602095DA39D70270938AE362F2DAE0 DD34020DD0804C0757F29A0CBBD7B46A1BAF949214F74FDFE

modulo n: Multiply by 5 times 11 times 21 | 1155, 483

20

0F1B1F946D327A4E9CA258C73A98F57 8559618EA2D83DF552D24EAF6BE983FB4AFB3DE7D4D254519 038EF55B4C826D189C6A48EFDD9DADBD2B63A7D675A0587C

Take the square modulo n:

25

30

8909DBBA1C04A6227FF18241C9FE E918EE6E99252DB3573CC87C604B327E5B20C7AB920FDF142A D1232F50E30BC6B7365CC2712E5CAE079E47B971DA03185B33

Multiply by 5 times 11 times 26 \parallel 1430, '596

F744C1FD751BFBCA040DC9CBAB744 984019BED9BF88247EF4CCB56D71E0FA30CFB0FF28B7CE45556 3CC768F12AEDFCD4662892B9174A21D1F0DD9127A54AB63C

Take the square modulo n:

0AE5ID90CB4FDC3DC757C56E063C9ED86BE153B71FC65F47C1 23C27F082BC3DD15273D4A923804718573F2F05E991487D17 DAE0AAB7DF0D0FFA23E0FE59F95F0

S successful. The commitment r is retrieved correctly. Authentication

Digital signature

S

controller to ascertain signed messages. Message M is any signing entity to produce signed messages and an entity called corresponding responses. binary sequence: it may be empty. The message M is signed by more The digital signing mechanism enables an entity called a commitments a signature appendix and/or challenges, to it, which comprises as well as the one or

10

15 in the signature appendix. controller by the demonstrator, for example by putting them parameters, i.e. numbers k, m and g_I to g_m may be given to the directory it also has the same hashing function. The GQ2 public The of public keys or even from a certificate of public controller has the module n, for example, from a

20 25 30 referenced from d_1 to d_m , as many as there are base numbers 2^{k-l} -1 (numbers v/2 to v-1 are not used). Each challenge challenge from d_1 to d_m on the one hand is a number from 0 to possible to sign with only one GQ2 triplet. For example, with kproduced in parallel; with $(k-1)\times m$ being 60 or more, it is Further, unless indicated otherwise, the m base numbers, 2,3,5,7,11,13,17 and 19. challenge includes eight bytes and the and m = g_m are the first m prime numbers. With $(k-1)\times m$ being Numbers k and m inform the controller. to 20, it is possible to sign with four GQ2 triplets hand should include ,8 only one GQ2 triplet m elementary challenges base numbers is sufficient; Each elementary from each

commitment act, a challenge act and a response The signing produces one operation or more isGQ2 triplets a sequence each comprising: of three act. Each act acts:

challenges referenced by $d_1, d_2, \dots d_m$ and a response $D \neq 0$. commitment $r \neq 0$, a challenge d consisting of m elementary

15 10 Ŋ private key, i.e., the factorization of the module n according order to isolate the most sensitive functions and parameters of n according to one of the three representations mentioned k and the GQ2 private key, i.e., the factorization of the module for example, • a chip card connected to a PC forming together demonstrator. it may correspond to a particular embodiment, isolated witness is similar to the witness defined within the one the three representations mentioned above. The thereby responses, the witness has the the demonstrator. In order chip card. witness which executes the commitment and response acts in within a PC, or even, • programs particularly protected within a the signing The signing entity has a hashing function, the parameter Within the signing entity, it is entity or even • programs particularly protected to compute commitments and parameter k and the GQ2 possible to isolate

operations 1) The act of commitment comprises the following

20

squarings (mode n), it transforms each random number r into random numbers r (0 < r < n); and then, by k successive and the module n, it randomly and privately picks one or more commitment R. When the witness has the m private numbers Q_I to

 $R \equiv r^{V} \pmod{n}$

includes a random number r_i per prime factor p_i (0 < r_i < p_i); random number r_i into a commitment component R_i , and then k successive squarings (mod p_i), it transforms each one or more collections of f random numbers: each collection $m \times f$ private When the witness components $Q_{I,j}$, it randomly and privately picks has f prime factors from p_1 to p_f and

30

25

 $R_i \equiv r_i^{V} \pmod{p_i}$

witness For each collection of f commitment components, establishes a commitment according to the Chinese

remainder are random number collections. technique. There are as many commitments as

 $r \equiv \text{Chinese remainders } (R_1, R_2, \dots R_f)$

Q

- 10 each elementary challenge is a number from 0 to v/2-1; for or more challenges each comprising m elementary obtain a hashing code from which the signing entity forms one commitments r and the message m to be signed in order bytes. There are as many challenges as there are commitments. example, = d_1 , d_2 , ... d_m , extracted from the Hash(M, R) result with k = 9 and m = 8, each challenge includes eight The act of challenge consists in hashing challenges; 0 1
- operations. The act of response includes the following

module n, it calculates one or more responses D by using each numbers according to the elementary challenges. random When the witness has m private numbers number r of the commitment act and the Q_{I} , to Q_{m} , and private

15

$$X \equiv Q_1^{d1} \times Q_2^{d2} \times \dots Q_m^{dm} \pmod{n}$$

of response factor of random numbers collections prime When the witness has f prime factors from p_1 to p_f and of f response components components from $D \equiv r \times X \pmod{n}$ components includes one component the commitment act; each $Q_{i,j}$ it calculates one by using each per collection collection prime

$$X \equiv Q_{1,i}^{d_1} \times Q_{2,i}^{d_2} \times \dots Q_{m,i}^{d_m} \pmod{p_i}$$
$$D_i \equiv r_i \times X_i \pmod{p_i}$$

25

20

challenges. technique. establishes For each collection of response a response There are according as many to the responses components, Chinese as the witness remainder there are

30

Chinese remainders $(D_1, D_2, ... D_f)$

signature appendix signing entity signs the message M by adding comprising ಬ

each challenge d and each response D, either each GQ2 triplet, i.e., each commitment χ,

response D, or each commitment R and each corresponding

response D. or each challenge d and each corresponding

S

on the contents of the signature appendix. Three The running of the verification operation depends cases are

10 conditions are satisfied. triplets, accepts the signed message if and only if, both following processes for which chronology is indifferent. The controller Should the appendix comprises the checking operation includes two independent one

acceptable (the comparison has to be done on a non-zero relationship Firstly, each triplet must be consistent (an appropriate of the following type has to be verified)

15

 $R \times \prod_{i=1} G_i^{d_i} \equiv D^{2^k}$ (mod n) or else $R \equiv D^{2^k} \times \prod G_i^{d_i} \pmod{n}$

20

commitment R present in the signature appendix. indicates whether it is necessary to use g_2 , ... up to the *i-th* bit th bit of the elementary challenge d_l indicates whether it is numbers. For the i-th multiplication or division which is of elementary operations: k squares (mod n) separated by k-lnecessary to use performed between the i-th square and the i+ 1st square, the imultiplication or division operations (mod n) by base necessary to use g_m . It is thus necessary For example, the response D is converted by a sequence elementary challenge g_L , the i-th bit of the elementary challenge d_m which indicates if to retrieve d_2

25

challenge Furthermore, the triplet or triplets must be linked to the M. d must be recovered. a hashing By hashing all the code is obtained commitments from which R and the

 $d = d_1 d_2...d_m$, identical to those extracted Hash(M, R). from the result

operation starts with the reconstitution of one or more challenges d^\prime by hashing all the commitments R and the message M. If the appendix has no challenge, the checking

Ŋ

 $d = d'_1 d'_2 \dots d'_m$, extracted from the result Hash(M, R).

the following type is verified) and acceptable (the comparison only if each triplet is consistent (an appropriate relationship of is done on a non-zero value). Then, the controller accepts the signed message if and

10

 $R \times \prod G_i^{d'_i} \equiv D^{2^k}$ Should the appendix comprise no commitment, (mod n) or else $R \equiv D^{2^k} \times \prod_{i=1}^{d^{d_i}} G_i^{d_i}$ (mod n)

15 the checking operation starts with the reconstitution of one or established commitment should be zero. formulae, namely the one more commitments R' according to one of the following two that is appropriate. No re-

 $R' \equiv D^{2^k} / \prod_{i=1}^m G_i^{d_i} \pmod{n} \text{ or else } R' \equiv D^{2^k} \times \prod_{i=1}^m G_i^{d_i} \pmod{n}$

message M so as to reconstitute each challenge d. Then, the controller must hash all the commitments R' and the

20

25

result Hash (M, R'). $d = d_1 d_2 \dots d_m$, identical to those extracted from the

challenge in the appendix. each reconstituted challenge The controller accepts the signed message if and only if is identical to the corresponding

1. Method designed to prove to a controller entity, authenticity of an entity and/or

by means - the integrity of a message M associated with this entity, of all or part of the following parameters or

derivatives of these parameters:

Ø

G₁, G₂, ... G_m (m being greater than or equal to 1), m pairs of private values Q₁, Q₂, ... Q_m and public values

of f

prime factors being related by relations of the following type the said modulus and the said private and public a public modulus n constituted by the $p_1, p_2, \dots p_f$ (f being greater than or product equal to 2), values

10

 G_i , $\equiv Q_i^{\ \nu}$, mod n or G_i , $\equiv Q_i^{\ \nu}$, mod n

where v denotes a public exponent of the form:

 $v = 2^k$

the said m public values G_i being squares g_i^2 of m distinct where k is a security parameter greater than 1; g₁, g₂, ... g_m, smaller than the f prime factors

р1,

15

base following conditions are satisfied: numbers the said p₁, p₂, ... p_m prime factors 81, g₂, ... g_m being produced and / or the said m such that the

condition

20

 $p_2, \dots p_m$; base numbers

each of the equations:

× × g: 2 mod n (1)

Second can be resolved in x in the ring of integers modulo n; condition

equal to $\pm g_i$ (in other words is not trivial), taking Qi squared modulo n, if $G_i \equiv Q_i^{\ \nu} \mod n$, among the m numbers k-1 times, one of them is q_i obtained by not

Ø

times, one of them is not equal to $\pm g_i$ (in other words is not taking the inverse trivial) if $G_i, Q_i^{\ \nu} \equiv 1 \mod n$, among the m numbers q_i obtained by of Q_i modulo n squared modulo **k** - 1

10 Third condition

at least one of the 2m equations $\frac{x^2}{2} = \frac{x^2}{2} = \frac{x^2}{$

 $x^2 \equiv g_i \mod n$ (2)

 $x^2 \equiv -g_i \mod n \quad (3)$

can be resolved in x in the ring of integers modulo n;

20 15 and/or the m private values Qi and/or the f.m components Qi,j remainders of the prime factors and/or the public modulus numbers of base entity called a witness having f prime factors pi and/or exponent v; $(Q_{i,j} \equiv Q_i \mod p_j)$ of the private values Q_i and of the public the said method implements, in the following steps, gi and/or parameters of the Chinese n

integers - the witness computes commitments modulo n; each commitment being computed: R in the ring οf

either by performing operations of the type:

 $R \equiv r^{v} \mod n$

25

30

where r is a random value such that 0 < r < n

. or

.. by performing operations of the type $R_i \ \equiv r_i{}^{\nu} \ mod \ p_i$

number P_i such that $0 < r_i < P_i$, each r_i belonging to a collection random values $\{r_1, r_2, \dots r_f\}$ where r_i is a random value associated with the prime

then by applying the Chinese remainders method,

challenge the witness receives comprising m integers one or more <u>d</u> challenges hereinafter d; each called

of the type: challenge d, computes elementary challenges; a response the witness, D by performing operations on the basis ofeach

 $D \equiv r.Q_1^{d1}.Q_2^{d2} \dots Q_m^{dm} \mod n$

. or

S

by performing operations of the type:

 $\overset{\longleftarrow}{D_i} \equiv r_i.Q_{i,1}{}^{d1}.\overset{\longleftarrow}{Q_{i,2}}^{d2}~...~Q_{i,m}{}^{dm}~mod~p_i$

then by applying the Chinese remainders method;

10 triplet referenced {R, d, D}. commitments R, each group of numbers responses the said method being U as there are such challenges that there R, d, D forming d as there are as many

15 comprising the authenticity known said demonstrator as Method according to claim 1, designed to prove of an entity known as a demonstrator to an entity the witness; controller, the said demonstrator and controller entities executing entity the the

Step 1: act of commitment R

following steps:

20

ЬУ applying the process - at each call, the witness computes each commitment specified according to claim 1, π

each commitment R, the demonstrator sends the controller all or part of

Step 2: act of challenge d

25

to the number of commitments R and sends the challenges commitment R, produces challenges the demonstrator, - the controller, after having received all or part of each d whose number is equal

. Step 3: act of response D

30

challenges d by applying the process claim 1, witness computes the responses specified according D from the 0

. Step 4: act of checking

35

controller, the demonstrator sends each response U Ö the

relationship of the type: response D, this reconstructed commitment R' satisfying reconstructed commitment R', from each challenge part of each commitment R if the demonstrator having the transmitted where the demonstrator a part of m public values G_1 , each commitment G₂ ..., G_m, computes has transmitted R, the d and each controller,

 $R' \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^v \mod n$

or a relationship of the type $R' \equiv D'/G_1^{dl}.G_2^{d2}...$

10

Ŋ

 2 G_m^{dm} . mod n

that has been transmitted to it, commitment R' reproduces controller ascertains all or part of each that each commitment reconstructed

15 totality of each commitment R where the demonstrator has transmitted the

relationship of the type commitment R, the controller, having the m public values if the demonstrator has transmitted G_m, ascertains that each commitment R satisfies the totality of each

or $R' \equiv G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot D^v \mod n$

20

a relationship of the type $R' \equiv D^{v}/G_1^{dl}.G_2^{d2}....G_m^{dm}. \mod n$

the witness; demonstrator entity, the proof to an entity, known as the integrity of a message M associated with an entity Method according to claim 1, designed said demonstrator controller entity entity, comprising to provide called a of the

25

following steps: said demonstrator and controller entities executing the

. Step 1: act of commitment R

30

bУ applying the process at each call, the specified according to claim 1, witness computes each commitment ∇

Step act of challenge

commitment R to compute at least one token T, arguments demonstrator applies are the message M and all a hashing or part function of h whose each

the demonstrator sends the token T to the controller,

commitments demonstrator, produces challenges d equal in number to the the controller, R and after sends having the challenges received a number Д Token ō the o f

. Step 3: act of response D

10

Ø

challenges d by applying the process claim 1, - the witness computes the responses specified according D from the to

. Step 4: act of checking

controller, the demonstrator sends each response U the

commitment R' satisfying a relationship of the type: challenge computes - the controller, having the m public values $G_1, G_2, ...,$ Q and reconstructed $R' \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^{v}$ each response commitment R', from Ų, mod n this reconstructed G_m ,

or a relationship of the type

20

15

25

 $R' \equiv D'/G_1^{dl}.G_2^{d2}....G_m^{dm}. \mod n$

- reconstructed commitment R' to reconstruct the token T', whose arguments the controller are the message M and all or applies the hashing part of each function
- identical to the token T transmitted. then the controller ascertains that the token
- Signing signing entity, the said signing entity comprising digital signature of a message M by 4. Method operation according to claim 1, designed to produce an entity known as the the witness; the

30

order to obtain a signed message comprising: said signing entity executes a signing operation

- the message M,

35

- the challenges d and/or the commitments R,

- the responses D;

implementing the following the said signing entity steps: executes the signing operation Ьу

Step 1: act of commitment R

S

- bу applying the process specified according to claim at each call, the witness computes each commitment ∇
- Step 2: act of challenge d
- obtain a binary train, arguments - the signing entity applies are the message M and a hashing each commitment function whose Rto

10

- commitments R, challenges from this binary train, whose number is equal the signing ō the number entity extracts o f
- Step 3: act of response D

15

- challenges d by applying claim - the witness computes the process the responses specified according J from the
- through an entity called a controller; authenticity of the message 5. Method according to claim 4, designed M by checking the signed message to prove
- Checking operation

20

a checking said controller entity having operation by proceeding as the signed message follows:

challenges where responses the controller has commitments D, ₹,

25

responses D, the controller has commitments , 기 challenges d,

challenges d and the responses D satisfy relationships .. the controller ascertains that the commitments of R, the the

 $R \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^v \mod n$

30

or relationships of the type $R \equiv D^{v}/G_1^{dl}.G_2^{d2}...G_m^{dm}. mod n$

challenges function the d controller and the commitments ascertains that the message \aleph satisfy the hashing M, the

Ф II h (message, R)

and responses . case U where the controller has challenges ۵

S

if the controller has challenges d and responses D,

relationships of the challenge the controller reconstructs, and response type: Ų, commitments on the basis of Ŋ satisfying

 $R' \equiv G_1^{d1}.G_2^{d2}$ 2 G_m^{dm} . D^v mod n

or relationships of the type

10

 $R' \equiv D^{v}/G_1^{d1}.G_2^{d2}....G_m^{dm}. \mod n$

challenges d satisfy the hashing function .. the controller ascertains that the message M and the

15

d=h(message,R')

and responses where U the controller has commitments Ħ

if the controller has commitments R and responses D,

reconstructs d' the controller applies the hashing function and

20

25

d' = h (message, R)

type: challenges d' and the responses . . the controller ascertains D satisfy relationships that the commitments of the R, the

 $R \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^v \mod n$

or relationships of the type $R \equiv D^{v}/G_1^{dl}.G_2^{d2}...G_m^{dm}. \text{ mod } n$

6 System designed to prove, to a controller server,

the authenticity

30

- the integrity of a message M associated with this entity,

of an entity and/or

derivatives of by means these parameters: of all or part of the following parameters

G₁,G₂, ... G_m (m being greater than or equal to 1), m pairs of private values Q1, Q2, ... Qm and public values

prime factors a public modulus n constituted by the product p_1 , p_2 , ... p_ℓ (f being greater than or equal to 2), of f

being the said modulus and the said private and public related by relations of the following type: values

 $G_i, Q_i^{\vee} \equiv 1$. mod n or $G_i \equiv Q_i^{\vee}$ mod n;

S

where v denotes a public exponent of the form:

 $v = 2^k$

where k is a security parameter greater than 1; the said m public values G_i being squares g_i^2 of m distinct base numbers $g_1, g_2, \dots g_m$, smaller than the f prime factors p_1, p_2, \dots

10

conditions are satisfied: numbers the said p₁, p₂, ... p_f prime factors and/or the said m base g₁, g₂, ... g_m being produced such that the following

First condition

15

each of the equations:

 $x_v \equiv g_i^2 \mod n$

can be resolved in x in the ring of integers modulo n;

Second condition

20

equal to $\pm g_i$ (in other words is not trivial). if $G_i.Q_i{}^{\nu}$ 1 mod n, among the m numbers q_i obtained $if G_i$ Q_i squared modulo n, Qi mod n, among the m numbers k-1 times, one of them is q_i obtained by not

taking the inverse trivial) times, one of them is not equal to of Qi modulo n squared modulo ±g_i (in other words is noı ьу

Third condition

25

at least one of the 2m equations

$$x^2 \equiv g_i \mod n \quad (2)$$

 $x^2 \equiv -g_i \mod n$ (3)

30

35

the

witness

device comprises

especially in a nomad object which, form of the can be resolved in x in the ring of integers modulo n; a microprocessor-based bank said system comprises a witness device, card, for example, contained takes the

the m numbers of bases gi and/or parameters of the Chinese remainders of the prime factors and/or the public modulus n and/or the m private values Qi and/or the f.m components exponent v; $(Q_{i,j} \equiv Q_i \mod p_j)$ of the private values Q_i and of the public a memory zone containing the f prime factors pi and/or

the said witness device also comprises:

Ŋ

random value production means of the witness random value production means, hereinafter called

computation of commitments R of the each commitment being computed: compute - computation means, hereinafter called means for commitments R in the ring of integers witness modulo device, 0 n;

10

• either by performing operations of the type:

 $R_i \equiv r^v \mod n$

15

production means, and r is such that 0 < r where r is a random value produced by the random value

or by performing operations of the type :

 $R_i \equiv r_i^{\vee} \mod p_i$

20

number p_i such that $0 < r_i < p_i$ each r_i belonging to a collection production means, of random method; where r_i is a random value associated with the values then by applying the Chinese $\{r_1, r_2,... r_f\}$ produced by random remainders value prime

25 the said witness device also comprises:

reception of the challenges d of the witness device, to receive integers di hereinafter called elementary challenges; or more challenges d; each challenge d comprising m - reception means hereinafter called the means for the

computation, on the basis of each challenge d, of a response computation of the responses D of the witness device for the computation means, hereinafter called means for the

30

either by performing operations of the type: $D \equiv r.Q_1^{d1}.Q_2^{d2}....Q_m^{dm} \mod n$

or by performing operations of the type: $D \equiv r.Q_{i,1}^{d1}.Q_{i,2}^{d2}....Q_{i,m}^{dm} \mod p_i$

and then by applying the Chinese remainders method.

commitments R and one or more responses D; there are - transmission means to transmit as many responses D as there are challenges one or more das

S

- forming a triplet referenced {R, d, D}. are commitments R, each group of numbers U
- 10 authenticity of an entity called a demonstrator called a controller, 7. System according to claim 6, designed and an entity to prove

the said system being such that it comprises:

- 15 interconnected demonstrator microprocessor in a microprocessor-based bank card, microcircuits in a nomad object, for example the form of a and possibly taking the demonstrator with the witness entity, the said device demonstrator device by interconnection form especially associated device with of being
- 25 20 entity, the said controller device especially taking the form of through electromagnetic, optical demonstrator terminal or controller device data-processing device; connection remote server, or communications network, to the associated with the controller means acoustic the said controller device connection, for its especially electrical,

the said system enabling the execution of the following

. Step 1: act of commitment R

30 of the witness device at each call, the means of computation for the commitments process specified according to claim 1, compute each commitment R by applying

device, to transmit all or part of each commitment R to the hereinafter demonstrator witness called device the transmission means device through has the means interconnection means, ofof the transmission, witness

controller device through the connection means; device, to transmit all or part of each commitment hereinafter called the transmission means of the demonstrator demonstrator device also has transmission R to means the

. Step 2: act of challenge

Ŋ

commitment R, of the number of commitments the controller for the production, device comprises challenge challenges ₽, after receiving d equal in number all or part of production to the each

hereinafter denoted transmission means transmit challenges means the controller d to the demonstrator through device also has transmission of the controller, connection means,

10

. Step 3: act of response D

15

device through the device receive each challenge d coming from the the means of reception of the challenges interconnection means, d of the witness demonstrator witness

applying the process specified according to claim device the means compute of computation of the responses the responses D from the D of the challenges 1, Q

ЬУ

. Step 4: act of checking

20

response transmission means to the controller, of the demonstrator transmit each

the controller device also comprises:

25

- means of the computation means, hereinafter controller device, called the computation
- comparison means, hereinafter controller device, called the comparison

each where the demonstrator has commitment transmitted ŋ part of

30

..., G_m, compute means transmitted of the controller device, having m public a part of each transmission means a reconstructed commitment of the commitment R, the demonstrator R', from values computation $G_1, G_2,$ have

commitment R' satisfying a relationship of the type: challenge Д and $R' \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^v$ each response D, mod n this reconstructed

or a relationship of the type $R' \equiv D^{v}/G_1^{d1}.G_2^{d2}....G_m^{dm}. \text{ mod } n$

Ŋ

commitment reconstructed commitment R' with all or part of each the comparison means of the controller device R received, compare

10 totality of each commitment R case where the controller has transmitted the

15 transmitted ascertain that each commitment R satisfies a relationship computation means and the comparison controller the transmission means type device, having m public the totality of ofeach commitment the values demonstrator $G_1, G_2,$ means of have the the

 $R \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^v \mod n$

or a relationship of the type $R \equiv D^{v}/G_1^{dl}.G_2^{d2}....G_m^{dm}. \text{ mod } n$

20 an entity known as a controller, of the integrity of a message M associated with an entity known as a demonstrator, said system being such that it comprises 8. System according lo claim 6, designed to give proof to

25 interconnected with demonstrator microcircuits in a nomad object, for example means and possibly taking the microprocessor in a microprocessor-based bank card, a demonstrator entity, the the witness device said demonstrator device being device form especially associated by interconnection the form of a with of logic the

electromagnetic, comprising entity, the said controller device especially taking the form of terminal controller or connection remote optical device server, the or associated with the controller means acoustic said connection, controller its electrical. especially device

demonstrator through a data processing device; communications network, ō the

steps: the said system enabling the execution of the following

. Step 1: act of commitment R

S

claim commitment R by applying the process specified according to commitments at each π call, of the the means of witness device computation compute ofeach the

10 transmit all or part of each commitment R called the transmission device the witness device through the interconnection means. has transmission means of the to the demonstrator means, witness hereinafter device,

. Step 2: act of challenge d

15

compute at least one token T, demonstrator, applying hereinafter the message the demonstrator device comprises called M and all or part of each commitment the a hashing function h whose arguments computation computation means means,

20 connection means demonstrator device, hereinafter the demonstrator device known to the as to transmit each token T through controller device, the transmission also has transmission means ofmeans, the the

challenges d in a number equal to the number of commitments controller device also has production, after having challenge received production means the token T, of the for

25

transmit the challenges hereinafter called the transmission connection means; controller device also d to the means of the demonstrator has transmission means, controller, through t o

30

Step 3: act of response L

device receive each device the means of reception of the challenges d through the challenge d coming from the interconnection means, of the demonstrator witness

applying the process specified according to claim 1, device compute the the means of computation of the responses responses D from the D of the witness challenges d by

Step 4: act of checking

Ø

each response the transmission means D to the controller, of the demonstrator transmit

satisfying a relationship of the type: device, having m public values G1, G2,..., Gm, in order d and each response compute hereinafter the controller device also comprises computation means, a called the computation reconstructed commitment R', from each challenge D, this reconstructed commitment means of the controller to firstly

10

 $R' \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^v \mod n$

a relationship of the

15

Or ionship of the type $R' \equiv D^{v}/G_1^{d1}.G_2^{d2}....G_m^{dm}. \mod n$

the known as the comparison means of the controller device, or part or each reconstructed commitment R', hashing function h having as arguments the message M and all controller device then, secondly, compute also has comparison means, hereinafter a token T' by applying the 0

20

signed message, by an entity called a signing entity; compare the token T' with the received token T. digital signature of a message System according to claim 6, designed to produce M, hereinafter known $\mathbf{a}\mathbf{s}$ the the

the signed message comprising:

25

- the message M,
- the challenges d and/or the commitments R,
- the responses D;

Signing operation

30 35 interconnected with the associated with the signing entity, the said signing device being microprocessor in microcircuits said system being such that it comprises and possibly taking in a nomad object, microprocessor-based bank witness device the for example the form form especially by interconnection a signing device card, of

the said system enabling the execution or the following steps:

. Step 1: act of commitment R

claim commitment R by applying the process specified according to commitments 1, at each R of the call, the means witness device of computation compute each the

S

signing device device, to transmit all or part of each commitment hereinafter witness called through the interconnection means, the transmission means of the device has means oftransmission, R to witness

Step 2: act of challenge d

10

whose number is equal to the number of commitments R, message M and all or part of each commitment R to compute hereinafter binary the train and extract, from this applying a hashing function h whose arguments signing called the computation device comprises binary train, computation means of the challenges are the signing means,

15

. Step 3: act of response D

each interconnection challenge d coming from the signing device through the the means for the reception of the challenges d, receive means,

20

applying the process specified according to claim 1, device compute the means for computing the responses the responses D from the D of the witness challenges d by

hereinafter called means of transmission of the witness device, interconnection to transmit the responses D to the signing device through the the witness device comprises means. transmission means,

25

30 by means of an entity called the controller; authenticity of the message 10. System according to claim 9, designed to prove M by checking the signed message the

Checking operation

35

device device the said system being such that it comprises a controller associated with the controller entity, the said controller especially taking the form of a terminal or.

communications connection, means for its electrical, electromagnetic, said controller network, especially to the signing through device comprising device; optical or data-processing connection acoustic

- to the controller transmission means of the signing device, for the transmission, comprises transmission means, hereinafter known connection means, signed message comprising: the said signing device associated with the signing entity device, in such a way that the controller device of the signed message through has the
- the message M,

10

Ŋ

- the challenges d and/or the commitments R.
- the responses D;

the controller device comprises:

- 15 means - computation means hereinafter of the controller device, called the computation
- means of the comparison means, hereinafter controller device. called the comparison

commitments case ₽, where challenges the d, controller responses U device has

20

responses D, if the controller has commitments R, challenges d,

25 challenges. controller the d and the device computation ascertain that the commitments responses D satisfy relationships and comparison means ofŖ, ofthe the the

 $R \equiv G_1^{d1}.G_2^{d2}.$ \dots G_m^{dm} . D^v mod n

or a

relationship of the type $R \equiv D^{v}/G_1^{dl}.G_2^{d2}....G_m^{dm}. \text{ mod } n$

30 controller device ascertain that the message M, the challenges d and the the commitments R satisfy the hashing computation and comparison function: means of the

= h (message, R)

Ω and case responses where the controller device has challenges

commitments R' satisfying relationships of the type: $R \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^v \mod n$ the basis of . . the if the controller device has challenges d and responses computation means of the each challenge d and each response D, compute controller device, Ų,

or a relationship of the type Ŋ

 $R \equiv D^{v}/G_1^{dl}.G_2^{d2}.$ \dots G_m^{dm} mod n

challenges d satisfy the hashing function: controller the device computation and comparison ascertain that the message means Z and of the the

d = h (message, R')

10

commitments case where Ħ and responses the device controller has commitments J device π has and

responses D, .. the computation means of the controller the controller device apply

15

the

hashing function and compute d' such that = h (message, R)

20 challenges controller the computation d' and the responses D satisfy relationships device ascertain that and comparison the commitments means of ofthe the the

 $R \equiv G_1^{d1}.G_2^{d2}...G_m^{dm}.D^v \mod n$

or ٦

25

relationship of the type $R = D^{v}/G_1^{d1}.G_2^{d2}....G_m^{dm}.$ '. mod n

- the designed to prove to a controller device: microprocessor in a microprocessor-based form especially of a nomad object, for example the form of Terminal device associated with an entity, taking bank card,
- the authenticity of an entity and/or

30

the integrity of a message M associated with this entity;

derivatives of these parameters: by means of all or part of the following parameters o r

 $G_1, G_2, ... G_m$ (m being greater than or equal to 1), m pairs of private values Q₁, Q₂, ... Q_m and public values

prime factors the said modulus and the said private and public values a public modulus $p_1, p_2, ..., p_f$ (f being greater than or equal to 2), n constituted by the product of f

being related by relations of the following type

 $Gi.Q_i^v \equiv 1 \mod n \text{ or } Gi \equiv Q_i^v \mod n;$

S

where

v denotes a public exponent of the form:

 $v=2^k$

the said where k is m public values Gi being squares gi2 of m distinct a security parameter greater than

10 base numbers numbers the said g₁, g₂, ... g_m, smaller than the f prime factors p₁, p₁, p₂, ... p_f prime factors being produced and / or the such that said m the

following conditions are satisfied: $g_1, g_2, \dots g_m$

First condition

15

each of the equations:

× $g_i^2 \mod n$

can be resolved in x in the ring of integers modulo n

Second condition

20 equal to $\pm g_i$ (in other words is taking if $Gi \equiv Q_i^{\text{v}} \mod n$, among Qi squared modulo n, not trivial), k-1 times, one of them the m numbers q_i obtained 1snot Ъу

if $G_i, Q_i^{\ \nu} \equiv 1 \mod n$, among the m numbers q_i obtained by taking of them is not equal to $\pm g_i$ (in other words is not trivial); the inverse of Qi modulo n squared modulo n, k-1 times, one

Third condition

25

at least one of the 2m equations

 $x^2 \equiv g_i \mod n$ (2)

 $x^2 \equiv -g_i \mod n$ (3)

can be resolved in x in the ring of integers

30

modulo the said terminal device comprises а witness device

the comprising m numbers a memory zone containing the f prime factors pi and/or of bases g; and/or parameters of the Chinese

 $(Q_{i,j} \equiv Q_i \mod$ and/or the m private exponent v; remainders of the prime factors and/or the public modulus p_j) of the private values Q_i and of the public values Q_i and/or the f.m components

the said witness device also comprises:

S

random value - random production means of the witness value production means, hereinafter device, called

compute commitments computation each commitment being computation ofcommitments means, hereinafter called means for R in the ring of integers modulo computed: R of the witness device, the 0

10

• either by performing operations of the type $R \equiv r^{v} \text{mod } n$

production means, where r is a random value produced by the random and r is such that 0 < r < n. value

15

or by performing operations of the type:

 $R_i \equiv r_i^{\ \ \ } \mod p_i$

number p_i such that $0 < r_i < p_i$ each r_i belonging method; production random where means, $\mathbf{r_i}$ is values a then by applying the Chinese remainders random $\{r_l, r_2,... r_f\}$ produced value associated with the by random to a collection prime

20

the said witness device also comprises:

25 reception of the challenges d of the integers one or - reception means hereinafter called the means more challenges d; each challenge d comprising di hereinafter called elementary witness challenges; device, to receive for the

D, computation, computation of the responses computation on the means, hereinafter called basis of each challenge D of the witness d, of a response device means for the for the

30

either by performing operations of the type: $D \equiv r.Q_1^{d1}.Q_2^{d2}....Q_m^{dm} \mod n$

or by performing operations of the type: $D \equiv r.Q_{i,1}^{d1}.Q_{i,2}^{d2}....Q_{i,m}^{dm} \mod p_i$

and then by applying the Chinese remainders method.

commitments transmission R and one or more responses D; means to transmit one or more

forming a triplet referenced {R, d, D}. there are are as many responses commitments R, each group of numbers D as there are challenges R, d, as U

Ŋ

entity called a prove the authenticity of an entity called a demonstrator Terminal device according to claim 11, designed controller; 0 a n

10 15 the said demonstrator device being interconnected with the demonstrator device associated with the demonstrator entity, the said terminal device being such that it comprises especially of taking the form of logic microcircuits in a nomad microprocessor-based bank object, for example the form of a microprocessor in witness device by interconnection means card, and being capable

communications network, taking the form of a terminal or remote server; with the controller entity, the said controller device especially connection, the said demonstrator device also comprising connection for its electrical, especially electromagnetic, to the controller through a optical or acoustic device data-processing associated

20

following steps: the said terminal device enabling the execution of the

. Step 1: act of commitment R

25

30

commitment commitments claim 1, at each R by applying the process specified according to call, ofthe the means witness ofdevice computation compute ofeach the

device through the interconnection means, transmit all or part of each commitment R to the demonstrator - the witness device has transmission means, hereinafter transmission means of the witness device 0 1

hereinafter the demonstrator called the device transmission also has transmission means means, the

the controller device, through the connection means; demonstrator, to transmit all or part of each commitment Rto

response Steps 2 and 3: act of challenge d, act

o f

the witness device, the means of computation of the responses interconnection means device device challenges d by applying D of the witness device compute device claim 1, the means of reception or the challenges d of the witness through receive the each challenge the demonstrator connection means between between the demonstrator the process d coming from the device the specified according responses and through the controller D from device controller

10

S

. Step 4: act of checking

each response D to the controller that carries out the check. the transmission means of the demonstrator transmit

of a give proof to an entity, known as a controller, demonstrator, message Terminal device according to claim 11, designed to M associated with an entity known as a of the integrity

20

25

object, for example especially of taking the form of logic witness device by interconnection means and being demonstrator device associated with the demonstrator entity, microprocessor-based bank card, said the demonstrator said terminal device being the form of a microprocessor device being such that it comprises microcircuits interconnected with the in a nomad capable in a

communications network, to the controller device connection, with the controller means for its electrical, electromagnetic, optical or acoustic taking the form of a terminal or remote server; said demonstrator device comprising especially entity, the said controller device through data-processing connection associated especially

30

the said terminal device being used Ö execute the

following steps:

. Step 1: act of commitment R

claim 1; commitment R by applying the process specified according to commitments each R of the call, the means witness device of computation compute of

demonstrator device through the interconnection means, device, to transmit all or part of each commitment R to the hereinafter the witness called the transmission means of the device has means of transmission, witness

response Steps 2 and 3: act of challenge d, act

10

S

demonstrator, applying a hashing function h whose arguments are the message M and all or part of each commitment hereinafter compute the demonstrator device comprises at least one token T, called the computation computation means, means Rto

connection means, to the controller device, demonstrator device, the demonstrator device known $\mathbf{a}\mathbf{s}$ to transmit each token T, through the the transmission also has transmission means ofmeans,

the token T), challenges d as the number of commitments R, after receiving (the said controller device produces the same number of

interconnection means between the demonstrator device controller device and the demonstrator device and device, through the device the witness device, the means of reception of the challenges d of the witness receive each challenge d coming interconnection means, from the controller between through the

25

30

20

15

by witness device compute the responses D from the challenges d applying means of computation of the responses D of the the process specified according to claim 1,

Step 4: act of checking

check. response transmission means of the demonstrator send each J to the controller device which carries out the

known as the signed message, by an entity produce the digital signature Terminal device according to claim of a message called 11, designed M, hereinafter a signing

S

the signed message comprising

the message M,

10

- the challenges d and/or the commitments R

- the responses D;

ofof logic microcircuits in a interconnection means and possibly taking especially signing signing device a microprocessor in a microprocessor-based bank the said terminal device being such that it comprises device being interconnected with the witness associated with the nomad object, for example signing entity, device by card, the form the the said

S

especially through a data-processing communications network, its electrical, electromagnetic, optical or acoustic connection, to the controller device terminal or remote server; said controller device the said signing device comprising associated especially taking with the controller entity, connection means for the form of a

20

Signing operation

25

following the steps: said terminal device being used ō execute the

. Step 1: act of commitment R

commitment R by applying the process specified commitments transmit all or claim device 1, the witness has means at each through the interconnection means, the transmission R of the call, part of each commitment the means witness device means of transmission, of the of computation witness R to compute according to the hereinafter device, signing each the

30

35

Step

act

of challenge

message M and all or part of each commitment R to compute device, applying a hashing function h whose arguments hereinafter number is equal to the number of commitments R, train and extract, from this binary train, challenges signing called the computation device comprises means computation of the are the signing means,

<u>د</u>: act of response D

S

signing device through the interconnection means, the means for computing the responses specified according to claim 1, witness responses D from the challenges d by applying the process the means device receive for the reception of the challenges the D of the challenges witness device compute đ coming from d of the the

10

hereinafter called means of transmission of the witness device. interconnection means. transmit the responses D to the signing device, through witness device comprises transmission means, the

15

- designed to prove: terminal or remote Controller server associated with a controller entity, device especially taking the form of
- authenticity or an entity and/or

20

the integrity of a message M associated with this entity.

derivatives of these parameters: by means of all or part of the following parameters

- 25 than or equal to 1), - m pairs of public values $G_1, G_2, ... G_m$ (m being greater
- unknown to the controller device and the associated controller entity prime factors p_1 , p_2 , ... p_f (f being greater than or equal to 2), a public modulus n constituted by the product of f

being related by relations of the following the said modulus and the said private and type public values

 G_i , $Q_i^{\vee} \equiv 1$, mod n or $G_i \equiv Q_i^{\vee}$ mod n;

where < denotes a public exponent of the form: || 2k

35

where k is a security parameter greater than 1;

device, associated with the public value Gi; Q_i is a private value, unknown to the controller

 $p_2, \dots p_f$; base numbers $g_1, g_2, \dots g_m$, smaller than the f prime factors p_1 , the said m public values G_i being squares g_i^2 of m distinct

S

following conditions are satisfied: base numbers the said p₁, p₂, ... p_f prime factors and / or the said m g₁, g₂, ... g_m being produced such that the

10 First condition

each of the equations:

 $x_v = g_i^2 \mod n$ (1)

can be resolved in x in the ring of integers modulo

Second condition

20 15 the inverse of Qi modulo n squared modulo n, k-1 times, one if $G_i, Q_i^{\ \nu} \equiv 1 \mod n$, among the m numbers q_i obtained by taking equal to $\pm g_i$ (in other words is not trivial). taking of them is not equal to $\pm g_i$ (in other words is not trivial); if $Gi = Q_i^{\text{v}} \mod n$, among the m numbers Q_i squared modulo n, k-1 times, one of them is qi obtained not ЬУ

Third condition

at least one of the 2m equations

 $^2 \equiv g_i \mod n$ (2)

 $x^2 \equiv -g_i \mod n$ (3)

can be resolved in x in the ring of integers modulo n.

25

prove the authenticity of an entity called a demonstrator to entity called a Controller device according to claim 15, designed controller; a n t o

communications network, to a demonstrator device associated connection, the the said controller device comprising connection means electrical, demonstrator entity; especially electromagnetic, through optical data-processing acoustic

30

following the said controller device being used to execute the

challenge and " act 0f commitment Ŗ, act

all demonstrator device through the said controller device also has means or part of the commitments connection means, ablafor the reception coming from the of

hereinafter called elementary challenges. R, of the challenges commitments production, after receiving all or part of each commitment the controller device has challenge production means R, each challenge d in a number equal to the d comprising m integers number for o f

10

Ŋ

hereinafter called transmission means of the connection means; transmit the challenges d to the demonstrator the controller device also has transmission controller, through means, the

- 15 the said controller device Steps 3 and 4: act of response, act of checking also comprises:
- from the - means for the reception demonstrator device, through the connection means, of the responses U coming
- means of the controller device, computation means, hereinafter called the computation

20

means of the controller device, comparison means, hereinafter called the comparison

part of each commitment R. where the demonstrator has transmitted 2

25 30 satisfying a relationship of the type compute a reconstructed commitment R', from each challenge or the controller device, having m public received a part of each commitment R, the d and each if the reception response D, this reconstructed commitment means of the values G_1, G_2, \ldots demonstrator computation means have

 $R' \equiv G_1^{d_1} \cdot G_2^{d_2} \cdot \dots \cdot G_m^{d_m} \cdot D^v \mod n$

a relationship of the type $R' \equiv D^{\nu}/G_1^{dl}.G_2^{d2}....G_m^{dm}. \ mod \ n$

commitment R received, reconstructed the comparison means of the controller commitment R' with all or part device compare of each

totality case where of each commitment R the demonstrator has transmitted the

S

received the totality of each commitment R, the computation means if the reception means of the controller and the comparison means of the controller device, m public values G₁, G₂, ..., G_m ascertain device that have each

commitment R satisfies a relationship of the type : $R \equiv G_1^{d1}.G_2^{d2}.....G_m^{dm}. \ D^v \ mod \ n$

10

or a relationship of the type

 $R \equiv D^{\nu}/G_1^{d1}.G_2^{d2}$ 2 G_m^{dm} . mod n

the a integrity Controller device according to claim 15, designed to prove demonstrator, of a message M associated with an entity known

15

associated with the communications connection, the said controller device comprising connection means electrical, especially network, demonstrator entity, electromagnetic, through to а demonstrator optical a data-processing or acoustic device

following the said controller device enabling the execution steps: of the

Steps 1 and 2: act of commitment R, act

challenge reception of tokens said controller device Q T coming from the demonstrator device also has means

for

the

through the connection means,

25

30

20

challenges d in a number equal to the number of commitments elementary challenges R, each challenge production, the controller device has challenge production after having d comprising m integers, hereinafter received the token T, of the means called for

hereinafter controller called the device transmission also has means transmission of the controller means,

through device, to transmit the the connection means; challenges Ω Ö the demonstrator

hecking Steps w and 4 act 0f response Ů, act o f

the said controller device also comprises:

Ŋ

- means for reception of the means, the demonstrator device, responses through the D coming connection from
- computation reconstructed commitment R', from each challenge public and each response computation means satisfying a relationship of the type: $R' \equiv G_1^{d1}.G_2^{d2}...G_m^{dm}.D^v \mod r$ values G_1 , means, D, this $G_2, \ldots,$ of the reconstructed controller device, having m hereinafter G_m to firstly mod n commitment called compute the

or a relationship of the type

15

10

 $R' \equiv D^{v}/G_1^{dl}.G_2^{d2}....G_m^{dm}. \mod n$

or part of each reconstructed commitment R', the controller hashing function device then, also secondly, compute comprises h having as arguments the message a token ij by applying M and all the

20

- the received token T. means of the controller device, to compare comparison means, hereinafter caned the comparison the token T' with
- signed message; checking designed a signed message to prove Controller the authenticity of the device by means of an according message entity called to claim ЬУ

25

30 with a signing entity having a hashing function comprising: the signed message sent by a signing device associated h (message,

- the message M,
- the challenges d and/or the commitments F
- the response D;

operation

the connection communications connection, for signing signed the said controller device electrical, means, entity, the said controller device having received message especially network, to a signing device from electromagnetic, the signing through comprising optical 2 device, connection means associated data-processing through or acoustic with the

S

the controller device comprises

10

- means of the controller device, computation means, hereinafter called the computation
- means of the comparison controller device; means, hereinafter called the comparison

commitments case R, challenges where the d, controller responses has

15

responses if the Ų, controller has commitments Ŗ, challenges **д**

challenges controller d and the responses D satisfy relationships device . . the computation and comparison ascertain that the commitments means of**7**2, ofthe the the

20

 $\mathbf{R} \equiv \mathbf{G_1}^{\mathrm{d1}}.\mathbf{G_2}^{\mathrm{d2}}.$ \dots G_m^{dm} . D^v mod n

а

or.

relationship of the type $R \equiv D^{v}/G_1^{d1}.G_2^{d2}....G_m^{dm}. \text{ mod } n$

25 challenges d satisfy the hashing function controller the device computation ascertain and that the comparison message means M and ofthe the

d = h (message, R)

commitments the case controller Ħ where and responses device the controller has J commitments device π and has

30

responses

D.

the hashing function and compute d' such that .. the computation means of the controller device apply

h (message, R')

controller device ascertain that the commitments type: challenges d' and the responses D satisfy relationships of the the computation and comparison means ₽, the the

 $R \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^v \mod n$

Ŋ

or a relationship of the type $R \equiv D^{\nu}/G_1^{dl}.G_2^{d2}....G_m^{dm}. \text{ mod } n$



(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ EN MATIERE DE BREVETS (PCT) UE COOPÉRATION

A CONTROL OF THE PARTY OF THE P

71

(19) Organisation Mondiale de la Intellectuelle Propriété

Bureau international

(43) Date de la publication internationale 12 avril 2001 (12.04.2001)



(10) Numéro de publication internationale WO 01/26279

(51) Classification internationale des brevets7: H04L 9/32

(21) Numéro de la demande internationale:

PCT/FR00/02717

dépôt international:

29 septembre 2000 (29.09.2000)

Langue de dépôt:

français français

9 Langue de publication:

(30) Données relatives à la priorité: 00/09644 99/12468 99/12467 99/12465 1 octobre 1999 (01.10.1999) 1 octobre 1999 (01.10.1999) 21 juillet 2000 (21.07.2000) octobre 1999 (01.10.1999) KKKK

(71) Déposants (pour FRANCE TELECOM [FR/FR]; 6. place d'Alleray, F-75015 Paris (FR). TELEDIFFUSION DE FRANCE F-75732 Paris Déposants (pour tous les États FRANCE TELECOM [FR/FR]; 'n [FR/FR]; 10, rue d'Oradour-sur-Glane, F-75732 Paris Cedex 15 (FR). MATH RIZK [BE/BE]; Verte Voie, Boîte B-1348 Louvain-la-Neuve (BE).

(72) (75) Inventeurs; et

Inventeurs/Déposants (pour US seulement): GUILLOU, Louis [FR/FR]; 16, rue de l'Ise, F-35230 Bourgbarre (FR).

QUISQUATER, Jean-Jacques [BE/BE]: 3, avenue Canards, B-1640 Rhode Saint Genese (BE). des

(74) Mandataire: VIDON, Patrice; Le Nobel, 2, allée Antoine Becquerel, BP 90 333, F-35703 Rennes Cedex 7 (FR).

(18) États désignés (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LK, LS, LT, LU, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(£8) États désignés (régional): brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen MO, GA, GN, GW, ML, MR, NE, SN, TD, TG). (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU NL, PT, SE), brevet OAPI (BF, BJ, CF, CG, CI, CM

Publiée:

Avec rapport de recherche internationale

abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT. tions, se référer aux "Notes explicatives relatives aux codes ce qui concerne les codes à deux lettres et autres abrévia-

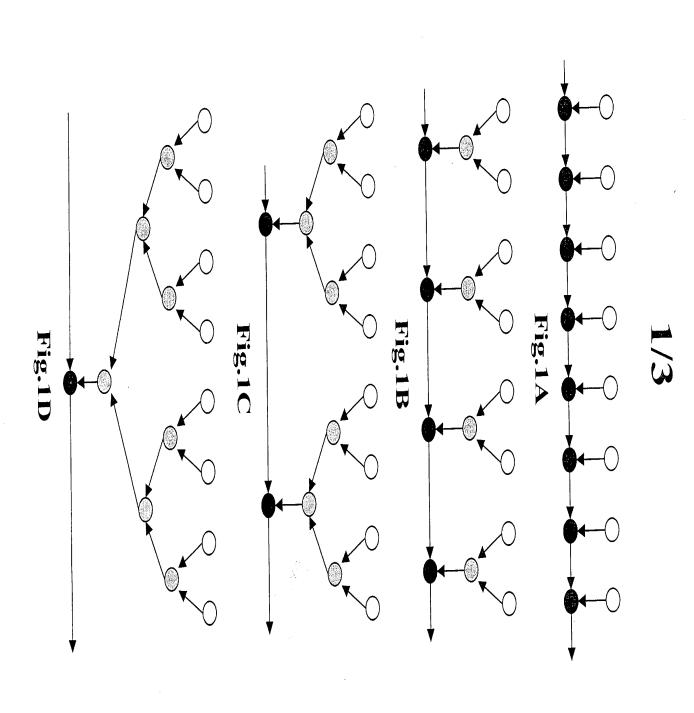
(54) Title: METHOD, SYSTEM, DEVICE FOR PROVING AUTHENTICITY OF AN ENTITY OR INTEGRITY OF A MESSAGE

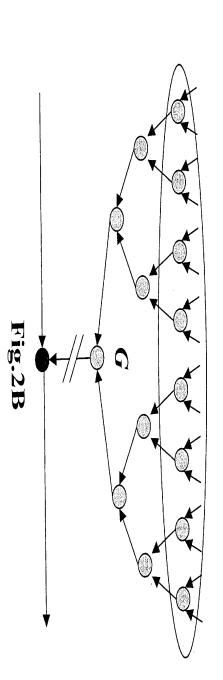
(54) Titre: PROCEDE, SYSTEME, DISPOSITIF A PROUVER L'AUTHENTICITE D'UNE ENTITE OU L'INTEGRITE D'UN

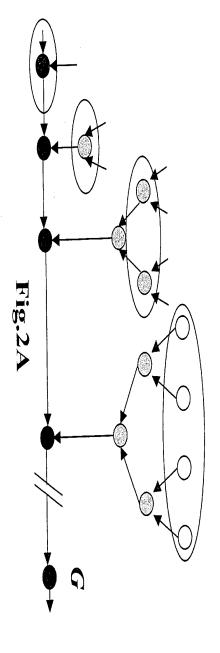
values; a public module n formed by the product of f(≥ 2) prime factors; an exponent $v = 2^k (k > 1)$, linked by the relationships of the type: $G_i . Q_i^v \equiv 1$. mod n or $G_i \equiv Q_i^v \mod n$. Among the m numbers obtained by increasing Q_i or its inverse modulo n to modulo n square, k-1 times rank, at least one of them is different from $\pm g_i$. Among the 2m equations: $x^2 \equiv g_i \mod n$, $x^2 \equiv -g_i \mod n$, at least one of them has solutions in x in the ring of modulo n integers. (57) Abstract: The invention concerns a method whereby the proof is established by: $m \ge 1$) pairs of private Q, and public $G_i = g_i$

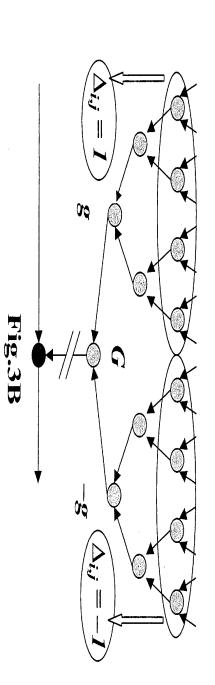
constitué par le produit de f (\geq 2) facteurs premiers, un exposant $v = 2^k$ (k > 1), liés par des relations du type: $G_i Q_i^v \equiv 1 \text{ mod n}$ ou $G_i \equiv Q_i^v \mod n$. Parmi les m nombres obtenus en élevant Q_i ou son inverse modulo n au carré modulo n, k-1 fois de rang, au moins l'un d'entre eux est différent de \pm g_i. Parmi les 2m équations: $x^2 \equiv g_i \mod n$; $x^2 \equiv -g_i \mod n$, au moins l'une d'entre elles a des (57) Abrégé: La preuve est établie au moyen de: m (\geq 1) couples de valeurs privées Q et publiques $G_i = g_i^2$, un module public n solutions en x dans l'anneau des entiers modulo n.

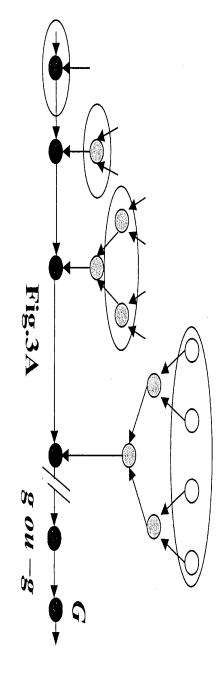
WO 01/26279











COMBINED DECLARATION AND POWER OF ATTORNEY IN ORIGINAL APPLICATION

Attorney Docket No.

F40.12-0007

SPECIFICATION AND INVENTORSHIP IDENTIFICATION

sought, sought, expricity ENTICITY ENTICITY characteristics characteri	s a below named inventor, I declare that: My residence, post office address and citizenship are as stated
--	--

ACKNOWLEDGEMENT OF REVIEW OF PAPERS AND DUTY OF CANDOR

I have reviewed and understand the contents of the above identified application, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is known to me to be material to the patentability of this application in accordance with 37 C.F.R. § 1.56.

PRIORITY CLAIM (35 U.S.C. § 119)

Prior Foreign Application(s)

I claim foreign priority benefits under 35 U.S.C. § 119(a-d) of any foreign application(s) for patent or inventor's certificate listed below, each of which is incorporated by reference in its entirety, indentified below any incorporated by reference in its entirety, and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

		,	
Number	Country	Day/Month/Year Filed	Priority Claimed
FR99 12465 FR99 12467	France	1 October 1999 1 October 1999	Yes X No
FR99 12468 FR00 09644	France	1 October 1999 21 July 2000	××

Prior Provisional Application(s)

I hereby claim the benefit under 35 U.S.C. States Provisional Application(s) listed below, each of by reference in its entirety: S119(e) o 0 f f any United incorporated

Day

Day/Month/Year Filed

PRIORITY CLAIM (35 U.S.C. ζ'n 120)

application(s) listed below, each of which is incorporated by reference in its entirety. Insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of 35 U.S.C. S 112, I acknowledge the material to patentability as defined in 37 C.F.R. S 1.56 which became available between the filing date of this application:

U.S. Appl. (if any un ol. No. under PCT) Filing Date

Status

DECLARATION

I declare that all statements made herein that are of my own knowledge are true and that all statements that are made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. § 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY

patent application identified above and to transact all business in the Patent substitution and revocation:

Kelly, Reg. No. 34,847; Nickolas E. Westman, Reg. No. 20,147; Steven M. Kroeze, Reg. No. 36,188; David D. Brush, Reg. No. 34,557; Theodore M. Kroeze, Reg. No. 38,354; Dairdre Megley Kvale, Reg. No. 38,354; Dairdre Megley Kvale, Reg. No. 35,612; Theodore M. Magee, Reg. No. 36,188; Christopher R. Christenson, Reg. No. 35,612; Brian D. Kaul 41,885; Robert M. Angus, Reg. No. 24,383; Christopher L. Holt, Reg. No. 45,844; Alan G. Rego, Reg. No. 45,956; and David C. Bohn, Reg. No. 32,015. Kroeze, Reg. No. 39,758; Ch Magee, Reg. No. 39,758; Ch Kaul. 41.885; Robert M. Ang Kaul. 41.885; Robert M. Ang business in the T

0 H 0 K the I ratify all prior actions taken by Westman, Champlin & attorneys and agents mentioned above in connection with the above-mentioned patent application. Relly, P.A. prosecution

DESIGNATION OF CORRESPONDENCE ADDRESS

calls

rt 0

Angus ij care Please re of: Phone address all correspondence and telephone WESTMAN, CHAMPLIN & KELLY, P.A. Suite 1600 - International Centre 900 Second Avenue South Minneapolis, Minnesota 55402-3319: (612) 334-3222 Fax: (612) 334 (612) 334-3312

(Signature)

Date:

Residence: Inventor: Louis Guillou (Printed, Na Name)

Address:

16,

rue

9

l'Ise,

Bourgbarre, France

Citizenship:

Bourgbarre, France

Inventor:

Date:

(Signature)

Rhode Saint Genese) Belgium & X <u>Jean-Jacques Quisquater</u> (Printed Name)

Inventor:

Residence: -

P.O. Address: 3, avenue des Canards, Rhode Saint Genese, Belgium 1640

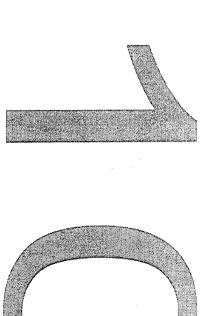
Citizenship:

Belgium

3-

UNITED STATES PATENT AND TRADEMARK OFFICE DOCUMENT CLASSIFICATION BARCODE SHEET

Miscollaneous



Level - 2 Version 1.1 Updated - 8/01/01

UNITED STATES PATENT AND TRADEMARK OFFICE DOCUMENT CLASSIFICATION BARCODE SHEET



371 Application Astrico

Level - 1 Version 1.1 Updated - 8/01/01

₩	June 19	
TRANSMITTAL LETTER DESIGNATED/ELECT	TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. § 371	Attorney Docket No. F40.12-0007
	(U.S. Application No. 707089662
INTERNATIONAL APPLICATION PCT/FR 06/02717	INTERNATIONAL FILING DATE 29.09.2000	PRIORITY DATE CLAIMED 01.10.99
THE OF BUILDING		!

METHOD, SYSTEM, DEVICE FOR PROVING AUTHENTICITY OF AN ENTITY OR INTEGRITY OF A MESSAGE

GIULLOU, Louis et al. APPLICANT(S) FOR DO/EO/US

	φ
	Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the followin
	ica
	nt
	he
	ře
	₹.
	ų,
	sut
1	Ħ
	its
	ö
	Ħ
	e [
,	ď
	Ę
}	ξ. Ω
	Sta
	tes
	Ü
	es
	69
	at
	еd
,	Ē
	ec
	tec
	10
•	Ħ
į	Ce
25 11 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	Ξ
	ŏ
١	Ē
1	9
1	Ğ
•	3
	he
	fo
	110
	₹.
	gn
	1
	m
	S
	nd
	o
	ns and other i
	E E
	afc
	П
	nat
	ior

- [X] This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
- This is a SECOND or SUBSEQUENT submission of items concerning a filing under 35 U.S.C. 371.
- W [X] This is an express request to begin national examination procedures (35 U.S.C. 371(f). The submission must include items (5), (6), (9) and (20) indicated below.
- 4. [X] The US has been elected by the expiration of the 19th month from the priority date (Article 31).
- [X] A copy of the International Application as filed (35 U.S.C. 371(c)(2))

'n

- [X] has been communicated by the International Bureau. [X] is transmitted herewith (required only if not transmitted by the International Bureau).
- [X] A translation of the International Application into English (35 U.S.C. 371(c)(2)). is not required, as the application was filed in the United States Receiving Office (RO/US).
- is attached hereto.
- has been previously submitted under 35 U.S.C. 154(d)(4).
- is not required, as the application was filed in English

7.

ò

- [X] Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3)) are attached hereto (required only if not transmitted by the International Bureau).
- have been transmitted by the International Bureau.
- 0 have not been made; however, the time limit for making such amendments has NOT expired
- have not been made and will not be made.
- A translation of the amendment to the claims under PCT Article 19 (35 U.S.C. 372(c)(3)).
- [X] An oath unexecuted or declaration of the inventor(s) (35 U.S.C. 371(c)(4)).
- Items 11. to 17. Below concern document(s) or information included: A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 37(c)(5)).

10.

- 11. [X] An Information Disclosure Statement under 37 CFR 1.97 and .198.
- 12. An assignment document for recording. A separate cover sheet in compliance with 37 C.F.R. 3.28 and 3.31 is included
- 13. [X] A FIRST preliminary amendment.
- 14. A SECOND or SUBSEQUENT preliminary amendment.
- 15. A substitute specification.
- 16. A change of power of attorney and/or address letter.
- 17. A second copy of the published international application under 35 U.S.C. 154(d)(4).
- 18. A second copy of the English language translation of the international application under 35 U.S.C. 154(d)(4).
- 19. [X] Other items or information: a.[X] Three (3) sheets of drawings.
- ь.[X] c. [X] File data sheet. Abstract typed on a separate page

U.S. APPLICATION NO. 10/089662 INTERNATIONAL APPLICATION NO. PCT/FR00/02717 F40.12-0007 ATTORNEY'S DOCKET NUMBER CALCULATIONS PTO USE ONLY

\$	charged				
\$	Amount to be: refunded				
	\$940	TOTAL FEES ENCLOSED =	TOTAL FEB		
	\$0	be accompanied +)). The assignment must be per property.	gnment (37 CFR 1.21(h) CFR 3.28, 3.31). \$40.00	Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property.
	\$0	TOTAL NATIONAL FEE =	TOTAL N.		
	\$0	[] 30	ater than [] 20	shing the English translationity date (37 CFR 1.4)	Processing fee of \$130.00 for furnishing the English translation later than months from the earliest claimed priority date (37 CFR 1.492(f))
	\$940	SUBTOTAL =			
	\$0	uced by 1/2.	fees indicated above are red	us. See 37 CFR 1.27. The	[] Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by 1/2
	\$0	LCULATIONS =	TOTAL OF ABOVE CALCULATIONS	7	
	\$0	+ \$270.00		(S) (if applicable)	MULTIPLE DEPENDENT CLAIM (S) (if applicable)
	\$80	X 80	1	4-3=	Independent claims
	\$0	X 18	О	18 - 20 =	Total claims
		RATE	NUMBER EXTRA	NUMBER FILED	CLAIMS
	\$0		ater than [] 20 [] 30 2(e)).	the oath or declaration I ority date (37 CFR 1.49)	Surcharge of \$130.00 for furnishing the oath or declaration later than [] 20 months from the earliest claimed priority date (37 CFR 1.492(e)).
	\$860	II	FEE AMOUNT	ENTER APPROPRIATE BASIC FEE AMOUNT	ENTER APPR
		\$ 100.00	and	ation fee paid to USPTO PCT Article 33(2)-(4)	International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2)-(4)
		.\$1000.00	82) nor	examination fee (37 CF 1.445(a)(2)) paid to US	Neither international preliminary examination fcc (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO
		0.00	PTO (37 CFR 1.482) but)(2))\$710.00	mination fee paid to USI SPTO (37 CFR 1.445(a	No international preliminary examination fee paid to USPTO (37 CFR 1.482) but international search fee paid to USPTO (37 CFR 1.445(a)(2))
		.00) (37 CFR 1.482) \$690.00	ation fee paid to USPTC	International preliminary examination fee paid to USPTO (37 CFR 1.482)
USE ONLY	CALCULATIONS PTO USE ONLY		\$860.00	re submitted: 1.492(A)(1)-(5)): by the EPO or JPO	20. [X] The following fees are submitted: BASIC NATIONAL FEE (37 CFR 1.492(A)(1)-(5)): Search Report has been prepared by the EPO or JPO

- a. [X] A check in the amount of \$940.00 to cover the above fees is enclosed.
- ъ. П A duplicate copy of this sheet is enclosed. Please charge my Deposit Account No. 23-1123 in the amount of \$ to cover the above fees.
- ; |X The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment, to Deposit Account No. 23-1123. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 C.F.R. 1.494 or 1.495 has not been met, a petition to revive (1.37(a) or (b)) must be filed and granted to restore the application to pending status.

Send all correspondence to:

Robert M. Angus
WESTMAN, CHAMPLIN & KELLY, P.A.
Suite 1600 - International Centre
900 Second Avenue South
Minneapolis, MN 55402-3319

Signature

Robert M. Angus

Reg. No.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

First Named Inventor : Louis Guillou et al.

Appln. No.:

Filed HEREWITH

For METHOD, METHOD, SYSTEM, DEVICE FOR PROVING AUTHENTICITY OF AN

F40.12-0007

ENTITY OR INTEGRITY OF A

MESSAGE

Docket No.:

Examiner: Group Art Unit:

PRELIMINARY AMENDMENT

EXPRESS MAIL NO. EV049900733US DATE OF DEPOSIT: March 29, 2002

Commissioner for Box Non-Fee Amendment Patents

Washington, D.C. 20231

Please amend the above-identified application

S follows:

THE SPECIFICATION

On Page 1, before line 1 and after the title,

please insert the following:

CROSS-REFERENCE TO RELATED APPLICATION

September 29, 01/26279, not in English. International Application No. PCT/FR00/02717 This Application is a Section 371 National Stage 2000, published April 12, 2001 as WO filed

FIELD OF THE INVENTION

the following: On Page 1, between lines 3 and 4, please insert

BACKGROUND OF THE INVENTION

the following: On Page 3, between lines 8 and 9, please insert

SUMMARY OF THE INVENTION

with the following: On Page 33, please delete line 12 and replace

BRIEF DESCRIPTION OF THE DRAWINGS

in explaining the present invention. FIGS. 1A-1D, 2A, 2B, 3A and 3B are graphs useful

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

IN THE CLAIMS

- 1. (Amended) Method designed to prove to a controller
- the authenticity of an entity and/or
- this entity, the integrity of a message M associated with

parameters or derivatives of these parameters: by means 0 fi all9 part Οf following

- equal to 1), values $G_1,G_2,\ \ldots \ G_m$ (m being greater than or m pairs of private values Q_1 , Q_2 , ...
- equal to 2), prime factors p_1 , p_2 , ... p_f (f being greater than or - a public modulus n constituted by the product of

values being related by relations of the following type the said modulus and the said private and public

 $G_i \cdot Q_i^{\ v} \equiv 1 \cdot \text{mod } n \text{ or } G_i \cdot \equiv Q_i^{\ v} \cdot \text{mod } n$

where v denotes a public exponent of the form:

where k is a security parameter greater than 1;

distinct base numbers g1, g2, ... gm, smaller than the f prime factors p1, p2, ... pm/; the said m public values $G_{f i}$ being squares ${g_{f i}}^2$ of m

m base numbers g1, g2, ... gm being produced such the said p1, p2, ... pm prime factors and/or following conditions are satisfied:

First condition

each of the equations:

$$x^v \equiv g_1^2 \mod n$$

modulo n; can be resolved in x in the ring of integers

Second condition

by taking Qi squared modulo n, k-1 times, one of them is not equal to ${}^{\pm}g_{\dot{1}}$ (in other words is not trivial), if $G_i \equiv Q_i^{\ V}$ mod n, among the m numbers q_i obtained

obtained by taking the inverse of Qi modulo n squared modulo n, k-1 times, one of them is not equal to $\pm 9i$ (in other words is not trivial); $G_{i} \cdot Q_{i}^{V} \equiv 1 \mod n$, among the m numbers

Third condition

at least one of the 2m equations

$$x^2 \equiv g_{imod} n$$

$$x^2 \equiv -gimod n$$

modulo n; can be resolved in x in the ring 0 Hi

parameters of the Chinese private values Qi and/or the f.m components Qi,j (Qi,j factors pi and/or m numbers of base gi and/or steps, an entity called a witness having f prime \equiv Q_i mod p_j) of the private values Q_i and of the public exponent v; the said method implements, in the following and/or the public modulus n and/or the m remainders of the

of integers modulo n; each commitment being computed: - the witness computes commitments R in the ring

. either by performing operations of the type:

 $R \equiv r^{v} \mod n$

where r is a random value such that 0 < r < n,

. or

.. by performing operations of the type

Ri ≡ri^v mod pi

prime number Pi such that 0<ri<Pi, each ri belonging to a collection of random values $\{r_1, r_2, \ldots, r_f\}$ ri is a random value associated with

performing operations of the type: each challenge d comprising m integers di hereinafter called elementary challenges; the witness, on the basis .. then by applying the Chinese remainders method, the witness receives one or more challenges d; challenge d, computes a response

 $D \equiv r.Q_1^{d1}.Q_2^{d2} ... Q_m^{dm} \mod n$

9

.. by performing operations of the type:

 $D_i = r_i \cdot Q_i, 1^{d_1} \cdot Q_i, 2^{d_2} \dots Q_i, m^{d_m} \mod p_i$

.. then by applying the Chinese remainders

triplet referenced {R,d,D}. commitments R, each group of numbers R, d, D forming a responses D as there are the said method being such that there are as many challenges d as there

prove the authenticity of an entity known as 2. (Amended) the said demonstrator and controller entities executing said demonstrator entity comprising the witness; demonstrator to an entity known as the controller, the the following steps: Method according to claim 1, designed to

. Step 1: act of commitment R

- according to claim 1, commitment R by at each call, the witness computes applying the process specified
- part of each commitment R, the demonstrator sends the controller all or

. Step 2: act of challenge d

part of each commitment R, produces challenges d whose number is equal to the number of commitments R and sends the challenges d to the demonstrator, controller, after having received all or

. Step 3: act of response D

challenges d by applying according to claim 1, the witness computes the responses the process U specified from the

. Step 4: act of checking

controller, the demonstrator sends each response U († 0 the

challenge d and each response D, this reconstructed controller, having the m public values G1, G2 ..., commitment R' satisfying a relationship of the type: transmitted each commitment case where the demonstrator has transmitted a part Ø reconstructed commitment R', from a part of each commitment **R** if the demonstrator the

 $R' \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^V \mod n$

or a relationship of the type

 $R' \equiv D^{v}/G_1^{d1}.G_2^{d2}. \dots G_m^{dm}. \mod n$

R that has been transmitted to it, commitment R' reproduces all or part of each commitment the controller ascertains that each reconstructed

case where totality of each commitment R the demonstrator has transmitted the

public values G_1 , G_2 ,... G_m , ascertains that commitment R satisfies a relationship of the type each commitment R, the controller, having the if the demonstrator has transmitted the totality

 $\texttt{R'} \equiv \texttt{G1}^{\texttt{d1}}.\texttt{G2}^{\texttt{d2}}. \ ... \ \texttt{Gm}^{\texttt{dm}}. \ \texttt{D}^{\texttt{V}} \ \texttt{mod} \ \texttt{n}$

or a relationship of the type

 $R' \equiv D'/G_1^{dl}.G_2^{d2}....G_m^{dm}. \mod n.$

Claims 3 and 4 are not changed.

prove the authenticity of the message M by checking the signed message through an entity called a controller; (Amended) Method according to claim 4, designed to

Checking operation

message executes a checking operation by proceeding as follows: the said controller entity having the signed

challenges d, responses D, case where the controller has commitments R,

responses D, if the controller has commitments R, challenges d,

relationships of the type the challenges d and the responses D the controller ascertains that the commitments satisfy

 $R \equiv G_1^{d1}.G_2^{d2}. \dots G_m^{dm}. D^V \mod n$

or relationships of the type

 $R \equiv D^V/G_1^{dl}.G_2^{d2}...G_m^{dm}. \mod n$

hashing function challenges d and the commitments R satisfy the the controller ascertains that the message M,

d = h (message, R)

and responses D case where the controller has challenges d

responses D, the controller has challenges Ω and

satisfying relationships of the type: challenge the controller reconstructs, d and response D, on the commitments basis

 $\texttt{R'} \equiv \texttt{G1}^{\texttt{d1}}.\texttt{G2}^{\texttt{d2}}. \; ... \; \texttt{Gm}^{\texttt{dm}}. \; \texttt{D^V} \; \texttt{mod} \; \texttt{n}$

or relationships of the type

 $R' \equiv D^{v}/G_1^{d1}.G_2^{d2}....G_m^{dm}. \mod n$

and the challenges d satisfy the hashing function the controller ascertains that the message Z

d=h (message,R')

responses D case where the controller has commitments R and

if the controller has commitments R and responses D,

and reconstructs d' the controller applies the hashing function

d' = h (message, R)

relationships of the type: the challenges d' and the responses the controller ascertains that the commitments U satisfy

 $R \equiv G_1^{d1}.G_2^{d2}. \dots G_m^{dm}. D^V \text{ mod } n$

or relationships of the type

 $R \equiv D^V/G_1^{d1}.G_2^{d2}....G_m^{dm}. \mod n.$

controller server, (Amended) System designed to prove, Ø

the authenticity of an entity and/or

this entity, - the integrity of a message M associated with

parameters or derivatives of these parameters: by means of all or part of the following

equal to 1), public values $G_1,G_2,\ldots G_m$ (m being greater than or m pairs of private values Q₁, Q₂, ... Q_m

equal to 2), f prime factors p_1 , p_2 , ... p_f (f being greater than or - a public modulus n constituted by the product of

values being related by relations of the following the said modulus and the said private and public

 $G_{i}.Q_{i}^{v} \equiv 1. \mod n \text{ or } G_{i} \equiv Q_{i}^{v} \mod n;$

where v denotes a public exponent of the form:

where k is a security parameter greater than 1;

prime factors p1, p2, ... pf; distinct base numbers g_1 , g_2 , ... g_m , smaller than the fsaid m public values $G_{\dot{1}}$ being squares ${g_{\dot{1}}}^2$

said m base numbers g1, g2, ... gm being produced such that the following conditions are satisfied: the said p1, p2, ... pf prime factors and/or

First condition

each of the equations:

$$x^v \equiv g_1^2 \mod n$$

modulo n; can be resolved in x in the ring of integers

Second condition

by taking Qi squared modulo n, k-1 times, one of them is not equal to $\pm g_i$ (in other words is not trivial), if $G_i \equiv Q_i^{V} \mod n$, among the m numbers q_i obtained

modulo n, k-1 times, one of them is not equal to $\pm 9i$ obtained by taking the inverse of Qi modulo n squared (in other words is not trivial); if $G_{\dot{1}}.Q_{\dot{1}}^{V} \equiv 1 \mod n$, among the m numbers

Third condition

at least one of the 2m equations

$$x^2 \equiv g_{imod n}$$

$$x^2 \equiv -g_{i} \mod n$$

modulo n; can be resolved in x in the ring of integers

example, takes the form of a microprocessor-based bank contained the said system comprises especially in a nomad מ object witness which,

the witness device comprises

- and/or the m numbers of bases gi and/or parameters public modulus n and/or the m private values $Q_{
 m i}$ and/or the said witness device also comprises: private values Q_i and of the public exponent v_i the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_{i} \mod p_{j}$) of the the Chinese remainders of the prime factors and/or the a memory zone containing the f prime factors
- called random value production means of the witness device, random value production means, hereinafter
- n; each commitment being computed: the computation of commitments R of the witness device, to compute commitments R in the ring of integers modulo computation means, hereinafter called means for
- either by performing operations of the type:

$$R_i \equiv r^{V} \mod n$$

value production means, and r is such that 0 < r < n; where r is a random value produced by the random

or by performing operations of the type:

prime number p_i such that $0 < r_i < p_i$ each r_i belonging 0 Ф where ri is a random value associated with the collection of random values {r1, r2,... rf}

applying the Chinese remainders method; produced by random value production means, then by

the said witness device also comprises:

- elementary challenges; challenge d comprising m integers di hereinafter called device, to receive one or more challenges d; each the reception of the challenges - reception means hereinafter called the means for d of the witness
- challenge d, of a response D, the computation of the responses D of the witness device for computation means, hereinafter called means the computation, on the basis of each
- . either by performing operations of the type:

 $D \equiv r.Q1^{d1}.Q2^{d2}. ... Qm^{dm} \mod n$

. or by performing operations of the type:

 $D = r.Qi, 1^{d1}.Qi, 2^{d2}...Qi, m^{dm} \mod pi$

method, and then by applying the Chinese remainders

- D forming a triplet referenced {R,d,D}. as there are commitments R, each group of numbers R, d, commitments R and one or more responses D; there are as many responses D as there are challenges d transmission means to transmit one or more
- demonstrator and an entity called a controller, 7. (Amended) authenticity of an entity called System according to claim 6, designed

the said system being such that it comprises:

demonstrator entity, the said demonstrator device being demonstrator device associated with the

interconnected microprocessor-based bank card, especially of logic microcircuits in a nomad object, interconnection means and possibly taking the form example the form of with the a microprocessor in witness

optical or acoustic connection, especially through a server, the said controller device comprising especially taking the form of a controller data-processing communications connection means for its electrical, electromagnetic, demonstrator device; controller device associated with the entity, the said controller network, terminal or remote the

following steps: the said system enabling the execution of the

. Step 1: act of commitment R

according to claim 1, commitment R by applying the process specified commitments R of the witness device compute each each call, the means of computation for the

witness device, to transmit all or part of each hereinafter called the transmission means commitment R to the demonstrator device through the interconnection means, witness device has means of transmission, of

demonstrator device, to transmit all or part of each means, hereinafter called the transmission means of the connection means; commitment the demonstrator device also has transmission R to the controller device through the

Step 2: act of challenge d

production means for the production, after receiving equal in number to the number of commitments R, all or part of each commitment R, of the challenges d controller device comprises challenge

demonstrator through connection means, controller, hereinafter the controller device also has transmission means, to transmit denoted transmission means challenges 0 fi

Step 3: act of response D

witness device receive each challenge d coming from the demonstrator device through the interconnection means, the means of reception of the challenges d of the

according to claim 1, challenges witness device compute the means of computation of the responses D of the d by applying the the process responses U

Step 4: act of checking

each response D to the controller, the transmission means of the demonstrator transmit

the controller device also comprises:

- computation means of the controller device, computation means, hereinafter called the
- comparison means of the controller device, comparison means, hereinafter the

each commitment R where the demonstrator has transmitted a part of

public values G_1 , G_2 , ..., G_m , compute a reconstructed commitment R', from each challenge d and each response computation means of the controller device, having m transmitted a part of each commitment if the transmission means of the demonstrator have R, the

relationship of the type: this reconstructed commitment R' satisfying

$$R' \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^V \mod n$$

or a relationship of the type

$$\texttt{R'} \equiv \texttt{D''}/\texttt{G_1}^{\texttt{d1}}.\texttt{G_2}^{\texttt{d2}}. \dots \texttt{G_m}^{\texttt{dm}}. \text{ mod n}$$

part of each commitment R received, compare each reconstructed commitment R' with all or comparison means of the controller

totality of each commitment R case where the controller has transmitted the

relationship of the type controller device, having m public values G1, G2, ..., computation means and the comparison means of the transmitted the totality of each commitment the transmission means of the demonstrator have ascertain that each commitment R satisfies

$$\mathbf{R} \; \equiv \; \mathbf{G1}^{\mathbf{d1}}..\mathbf{G2}^{\mathbf{d2}}. \; \; \mathbf{Gm}^{\mathbf{dm}}. \; \mathbf{D^{V}} \; \mathbf{mod} \; \mathbf{n}$$

or a relationship of the type

$$R \equiv D^V/G_1^{d1}.G_2^{d2}....G_m^{dm}. \mod n.$$

give proof to an entity known as a controller, 8. (Amended) integrity of a message M associated with an entity known as a demonstrator, System according to claim 6, designed to

the said system being such that it comprises

demonstrator entity, the said demonstrator device being interconnection means and possibly taking the interconnected with the especially of logic microcircuits in a nomad object, demonstrator device associated witness device

microprocessor-based bank card, example the form of a microprocessor in a

optical or acoustic connection, especially especially taking the form of a connection means for its electrical, electromagnetic, server, the said controller controller demonstrator device; processing communications controller device entity, the said associated with the device comprising terminal or remote controller network, through t 0 the

following steps: said system enabling the execution of the

Step 1: act of commitment R

according to claim 1, commitment R by applying the process specified commitments R of the witness device compute each at each call, the means of computation of the

witness device, to transmit all or part of hereinafter called the transmission means of the interconnection means, commitment R to the demonstrator device through the the witness device has transmission means,

Step 2: act of challenge d

means, hereinafter called the computation means of the commitment R to compute at least one token T, arguments are the message M and all or part of each demonstrator, applying a hashing function h whose the demonstrator device comprises computation

means, hereinafter known as the transmission means of demonstrator device also has transmission

the controller device also has challenge production through the connection means to the controller device, the demonstrator device, to transmit each token number of commitments R, token T, of the challenges d in a number equal to the for the production, after having received the

demonstrator through the connection means; controller, hereinafter called the the controller device also has transmission means, to transmit the challenges d transmission means O H

Step 3: act of response D

demonstrator device through the interconnection means, witness device receive each challenge d coming from the the means of reception of the challenges d of

witness device compute challenges d by according to claim 1, the means of computation of the responses D of the applying the responses the process U specified

. Step 4: act of checking

transmit each response D to the controller, transmission means 0 fi the demonstrator

relationship of the type: commitment R', from each challenge d and each response controller device, having m public values G1, G2,..., means, hereinafter called the computation means of the in order to firstly compute a reconstructed controller device also comprises computation reconstructed commitment R' satisfying

 $R' \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^V \mod n$

or a relationship of the type

 $R' \equiv D^{v}/G_1^{d1}.G_2^{d2}....G_m^{dm}. \mod n$

and all or part or each reconstructed commitment R', then, secondly, compute a token T' by applying the function h having as arguments the message M

controller device, to compare the token T' with the hereinafter known as the comparison means received token T. the controller device also has comparison means,

Claim 9 is not changed.

prove the authenticity of the message M by checking the 10. (Amended) System according to claim 9, designed to signed message by means of an entity called controller;

Checking operation

entity, the said controller device especially taking controller device associated with the controller electrical, controller device comprising connection means for its the form of a terminal or remote server, the said communications network, to the signing device; connection, especially through a data-processing the said system being such that it comprises electromagnetic, optical

means, in such a way that the controller device has a signing device, for the transmission, to the controller hereinafter known as the transmission means of signing signed message comprising: device, the of the said signing device associated with the entity signed message through the connection comprises transmission

- the message M,
- the challenges d and/or the commitments R,
- the responses D;

the controller device comprises:

- computation means of the controller device, computation means hereinafter the
- comparison means of the controller device; comparison means, hereinafter called the

R, challenges d, responses D case where the controller device has commitments

responses D, if the controller has commitments R, challenges d,

challenges d and the responses D satisfy relationships of the type controller device ascertain that the commitments R, the the computation and comparison means

$$R \equiv G_1^{d1}.G_2^{d2}. \dots G_m^{dm}. D^V \mod n$$

or a relationship of the type

$$R \equiv D^{v}/G_1^{d1}.G_2^{d2}...G_m^{dm}. \mod n$$

challenges d and the commitments R satisfy the hashing controller device ascertain that the message the computation and comparison means of

d = h (message, R)

d and responses D . case where the controller device has challenges

responses D, the controller device has challenges d and

device, on the basis of each challenge d and each the computation means of the controller

relationships of the type: response Ŭ, compute commitments Ħ

 $R \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^V \mod n$

or a relationship of the type

 $R \equiv D^{v}/G_1^{dl}.G_2^{d2}....G_m^{dm}. mod n$

challenges d satisfy the hashing function: controller device ascertain that the message M and the . . the computation and comparison means of the

d = h (message, R')

and responses D case where the controller device has commitments R

responses D, if the controller device has commitments R and

apply the hashing function and compute d' such that . the computation means of the controller device

d' = h (message, R)

challenges d' and the responses D satisfy relationships controller device ascertain that the commitments R, of the type: . . the computation and comparison means 0 f

 $R \equiv G_1^{d1}.G_2^{d2}. ... G_m^{dm}. D^V \text{ mod } n$

or a relationship of the type

 $R \equiv D^{v}/G_1^{d1}.G_2^{d2}....G_m^{dm}. \mod n.$

entity, taking the form especially of a nomad object, 11. (Amended) Terminal device microprocessor-based bank card, designed to prove to a for example the form controller device: of a microprocessor associated with

the authenticity of an entity and/or

this entity; the integrity of a message M associated with

parameters or derivatives of these parameters: by means of all 9 part of the following

1), values $G_1,G_2,\ \ldots \ G_m$ (m being greater than or equal to m pairs of private values $Q_1,\ Q_2,\ \ldots\ Q_m$ and public

f prime factors p_1 , p_2 , ... p_f (f being greater than or equal to 2), - a public modulus n constituted by the product

values being related by relations of the following type the said modulus and the said private and public $Gi.Q_i^{\ \ v} \equiv 1 \mod n \text{ or } Gi \equiv Q_i^{\ \ v} \mod n;$

where v denotes a public exponent of the form:

where k is a security parameter greater than 1:

prime factors p1, p2, ... pf; distinct base numbers g1, g2, ... g_m , smaller than the f the said m public values $G_{
m i}$ being squares ${g_{
m i}}^2$ of m

that the following conditions are satisfied: m base numbers said p1, p2, ... pf prime factors and/or g1, g2, ... gm being produced such

First condition

each of the equations:

 $x^v \equiv g_1^2 \mod n$

modulo n can 9 resolved in x in the ring ΟĦ integers

Second condition

by taking Qi squared modulo n, k-1 times, one of them is not equal to ${}^{\pm}\!g_i$ (in other words is not trivial), if $Gi \equiv Q_i^V \mod n$, among the m numbers q_i obtained

if $G_{i} \cdot Q_{i}^{V} \equiv 1 \mod n$, among the m numbers q_{i} obtained by times, one of them is not equal to +gi (in other words taking the inverse of Qi modulo n squared modulo n, k-1 is not trivial);

Third condition

at least one of the 2m equations

$$x^2 \equiv g_1 \mod n$$

$$x^2 \equiv -g_1 \mod n$$

can be resolved in x in the ring of integers

modulo n;

device comprising the said terminal device comprises a witness

and/or the m numbers of bases g_i and/or parameters of public modulus n and/or the m private values $Q_{
m i}$ and/or the Chinese remainders of the prime factors and/or the private values Q_i and of the public exponent v_i f.m components Q_i, j ($Q_i, j \equiv Q_i \mod p_j$) of the a memory zone containing the f prime factors

the said witness device also comprises:

- called random value production means of the witness random value production means, hereinafter
- the computation of commitments R of the witness device, computation means, hereinafter called means **HOT**

n; each commitment being computed: to compute commitments R in the ring of integers modulo

type: either by performing operations of the

 $R \equiv r^{V} \mod n$

value production means, and r is such that 0 < r < n. where r is a random value produced by the random

• or by performing operations of the type:

Ri = ri mod pi

prime number p_i such that $0 < r_i < p_i$ each r_i belonging applying the Chinese remainders method; produced by random value production means, then by a collection of random values $\{r_1, r_2, \dots r_f\}$ where ri is a random value associated with the

the said witness device also comprises:

- challenge d comprising m integers di hereinafter called elementary challenges; the reception of the challenges d of the - reception means hereinafter called the means for receive one or more challenges d; each witness
- the computation of the responses D of the witness challenge d, of a response D, computation means, hereinafter called means for for the computation, on the basis of each
- . either by performing operations of the type:

 $\mathbf{D} \equiv \mathbf{r}.\mathbf{Q}_1^{\mathbf{d}_1}.\mathbf{Q}_2^{\mathbf{d}_2}. \dots \mathbf{Q}_m^{\mathbf{d}_m} \bmod \mathbf{n}$

or by performing operations of the type:

 $D = r.Qi, 1^{d1}.Qi, 2^{d2}. ... Qi, m^{dm} mod pi$

method. then by applying the Chinese remainders

D forming a triplet referenced $\{R, d, D\}$. as there are commitments R, each group of numbers R, there are as many responses D as there are challenges d commitments R and one or more responses D; transmission means to transmit one or

Claims 12-14 are not changed.

15. (Amended) Controller device especially taking the controller entity, designed to prove: form of a terminal or remote server associated with a

- the authenticity or an entity and/or
- this entity. the integrity of a message M associated with

parameters or derivatives of these parameters: by means of all or part of the following

- greater than or equal to 1), m pairs of public values $G_1,G_2,\ \ldots \ G_m$ (m being
- equal to 2), unknown to the controller device and the associated controller entity, prime factors p_1 , p_2 , ... p_f (f being greater than or a public modulus n constituted by the product of

values being related by relations of the following type the said modulus and the said private and public

 G_i . ${Q_i}^v$ = 1. mod n or G_i = ${Q_i}^v$ mod n;

where v denotes a public exponent of the form:

where k is a security parameter greater than 1;

controller device, associated with the public value Gi; where Qi is a private value, unknown to the

prime factors p1, p2, ... pf; distinct base numbers g_1 , g_2 , ... g_m , smaller than the the said m public values $G_{
m i}$ being squares ${g_{
m i}}^2$ of m

said m base numbers g1, g2, ... gm being produced such that the following conditions are satisfied: the said p1, p2, ... pf prime factors and/or the

First condition

each of the equations:

$$\dot{x}^{v} \equiv g_{\dot{1}}^{2} \mod n$$

modulo n can be resolved in x in the ring of integers

Second condition

by taking Qi squared modulo n, k-1 times, one of them is not equal to ${}^{\pm}g_{\dot{1}}$ (in other words is not trivial), if $Gi \equiv Q_i^V \mod n$, among the m numbers q_i obtained

if $G_i \cdot Q_i^{\ V} \equiv 1 \mod n$, among the m numbers q_i obtained by times, one of them is not equal to +gi (in other words taking the inverse of Qi modulo n squared modulo n, k-1 is not trivial);

Third condition

at least one of the 2m equations

$$x^2 \equiv g_1 \mod n$$

$$x^2 \equiv -g_{imod}$$

modulo n. be resolved in x in the ring 0 Ħ integers

designed to prove the authenticity of an entity called 16. (Amended) Controller device according to claim 15, a demonstrator to an entity called a controller;

means for its electrical, electromagnetic, optical or device associated with the demonstrator entity; processing communications network, to acoustic connection, especially the said controller device comprising connection through a demonstrator

the following steps: said controller device being used to execute

challenge d Steps 1 and 2; act of commitment R, act

reception of all or part of the commitments R coming means, from the demonstrator device through the connection said controller device also has means for the

means for the production, after receiving all or part comprising m integers di hereinafter called elementary equal to the number of commitments R, each challenge of each commitment R, of the challenges d in a number challenges, the controller device has challenge production

controller, hereinafter demonstrator through the connection means; the controller device also has transmission means, to transmit called transmission the challenges means 0 fi the the

Steps 3 and 4: act of response, act of checking

the said controller device also comprises:

connection means, means tor the the reception of demonstrator device, the through responses the

- computation means of the controller device, computation means, hereinafter the
- comparison means of the controller device, comparison means, hereinafter called the

of each commitment R case where the demonstrator has transmitted a part

 G_1 , G_2 , ..., G_m compute a reconstructed commitment R', means or the controller device, having m public values received a part of each commitment R, the computation reconstructed commitment R' satisfying a relationship of the type: from each challenge d and each response D, this if the reception means of the demonstrator have

 $\texttt{R'} \equiv \texttt{G1}^{\texttt{d1}}.\texttt{G2}^{\texttt{d2}}. \ ... \ \texttt{Gm}^{\texttt{dm}}. \ \texttt{D^V} \ \texttt{mod} \ \texttt{n}$

or a relationship of the type

 $\texttt{R'} \equiv \texttt{D'}/\texttt{G_1}^{\texttt{d1}}.\texttt{G_2}^{\texttt{d2}}. \dots \texttt{G_m}^{\texttt{dm}}. \text{ mod n}$

part of each commitment R received, compare each reconstructed commitment R' with all or comparison means of the controller device

totality of each commitment R case where the demonstrator has transmitted the

have received the totality of each commitment relationship of the type: controller device, having m public values G1, G2, ..., computation means ascertain that each commitment R satisfies if the reception means of the controller device and the comparison means of

 $R \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^V \mod n$

or a relationship of the type

 $R \equiv D^{v}/G_1^{d1}.G_2^{d2}....G_m^{dm}. \mod n.$

Claim 17 is not changed.

designed to prove the authenticity of the message M by 18. (Amended) Controller device according to claim 15, checking a signed message by means of an entity called a signed message;

associated with a signing entity having a hashing function h (message, R), comprising: the signed message sent by a signing device

- the message M,
- the challenges d and/or the commitments R,
- the response D;

Checking operation

processing communications network, to a signing device means for its electrical, electromagnetic, optical or associated with the signing entity, the said controller acoustic signing device, through the connection means, device having received the signed message connection, especially said controller device comprising connection through מ from the

the controller device comprises:

- computation means of the controller device, computation means, hereinafter the
- comparison means of the controller device; comparison means, hereinafter the

challenges d, case where the controller device has commitments responses D

responses D, if the controller has commitments R, challenges d,

the controller device ascertain that the commitments R, relationships of the type challenges d and . . the computation and comparison means the responses U

 $\mathbf{R} \ \equiv \ \mathbf{G_1}^{\mathbf{d1}}.\mathbf{G_2}^{\mathbf{d2}}. \ \dots \ \mathbf{G_m}^{\mathbf{dm}}. \ \mathbf{D^V} \ \mathbf{mod} \ \mathbf{n}$

or a relationship of the type

 $R \equiv D^{v}/G_1^{d1}.G_2^{d2}....G_m^{dm}. mod n$

controller device ascertain that the message M and the challenges d satisfy the hashing function . the computation and comparison means of the

d = h (message, R)

case where the controller device has commitments

R and responses D

if the controller device has commitments R and

apply the hashing function and compute d' such that . the computation means of the controller device

d' = h (message, R')

challenges d' and the responses D satisfy relationships controller device ascertain that the commitments R, the of the type: . the computation and comparison means of the

 $R \equiv G_1^{\text{dl}}.G_2^{\text{d2}}. \dots G_m^{\text{dm}}. D^V \text{ mod } n$

or a relationship of the type

 $R \equiv D^{v}/G_1^{d1}.G_2^{d2}...G_m^{dm}. \mod n.$

REMARKS

Favorable action is respectfully requested.

deficiency overpayment to Deposit Account No. 23-1123. The Director is authorized to charge any fee required by this paper or credit

Respectfully submitted,

WESTMAN, CHAMPLIN & KELLY, P.A.

By: Minneapolis, Minnesota 55402-3319 Phone: (612) 334-3222 Fax: (612) 900 Second Avenue South Robert M. Angus, Reg. No. 24,383
Suite 1600 - International Centre Fax: (612) 334-3312

RMA: tas

MARKED UP VERSION OF REPLACEMENT CLAIMS

- entity, 1. (Amended) Method designed to prove to a controller
- the authenticity of an entity and/or
- this entity, the integrity of a message M associated with

parameters or derivatives of these parameters: by means of all or part of the

- public values $G_1,G_2,\ \ldots \ G_m$ (m being greater than or equal to 1), m pairs of private values Q_1 , Q_2 , ...
- equal to 2), prime factors p_1 , p_2 , ... p_f (f being greater than or - a public modulus n constituted by the product of

values being related by relations of the following type the said modulus and the said private and public $G_i.Q_i{}^{V} \equiv 1$. mod n or $G_i. \equiv Q_i{}^{V}$. mod n

where v denotes a public exponent of the form:

where k is a security parameter greater than 1;

prime factors p1, p2, ... pm|; distinct base numbers g_1 , g_2 , ... g_m , smaller than the fthe said m public values $G_{f i}$ being squares ${g_{f i}}^2$ of m

that the following conditions are satisfied: m base numbers g1, g2, ... gm being produced such the said p1, p2, ... pm prime factors and/or

First condition

each of the equations:

$$x_{\psi^{\underline{v}}} \equiv g_{\underline{i}}^2 \mod n + (1)$$

modulo n; can be resolved in x in the ring of integers

Second condition

is not equal to ${}^{\pm}g_{1}$ (in other words is not trivial), by taking Qi squared modulo n, k-1 times, one of them if $G_i \equiv Q_i^{\ V}$ mod n, among the m numbers q_i obtained

modulo n, k-1 times, one of them is not equal to $\pm 9i$ obtained by taking the inverse of Qi modulo n squared (in other words is not trivial); if $G_i \cdot Q_i^V \equiv 1 \mod n$, among the m numbers

Third condition

at least one of the 2m equations

$$x^2 \equiv g_{i} \mod n + (2)$$

$$x^2 \equiv -g_{imod n} + \frac{3}{3}$$

modulo n; can be resolved in x in the ring of integers

 \equiv Qi mod pj) of the private values Qi and of the public private values Qi and/or the f.m components Qi,j (Qi,j parameters of the Chinese remainders of the factors pi and/or m numbers of base steps, an entity called a witness having f prime factors exponent v; the said method implements, in the following and/or the public modulus n and/or the m gi and/or prime

- of integers modulo n; each commitment being computed: the witness computes commitments R in the ring
- either by performing operations of the type:

$$R \equiv r^{v} \mod n$$

where r is a random value such that 0 < r < n,

6

.. by performing operations of the type

 $R_i \equiv r_i^{\mathsf{v}} \mod p_i$

prime number Pi such that 0<ri<Pi, each ri belonging to a collection of random values $\{r_1, r_2, \ldots, r_f\}$ where ri is a random value associated with the

performing operations of the type: called elementary challenges; the witness, on the basis each challenge d comprising m integers di hereinafter each challenge d, computes a response .. then by applying the Chinese remainders method, the witness receives one or more challenges d;

 $D = r.Q_1^{d1}.Q_2^{d2} ... Q_m^{dm} \mod n$

. or

.. by performing operations of the type:

 $D_i = r_i.Q_i, 1^{d1}.Q_i, 2^{d2} \dots Q_i, m^{dm} \mod p_i$

.. then by applying the Chinese remainders

triplet referenced {R,d,D}. commitments R, each group of numbers R, d, D forming a responses D as there are challenges d as there are the said method being such that there are as many

prove the authenticity of an entity known as said demonstrator entity comprising the witness; demonstrator to an entity known as 2. (Amended) Method according to claim 1, designed to the controller, the

the said demonstrator and controller entities executing the following steps:

Step 1: act of commitment R

- according to claim 1, commitment R by applying р С† each call, the the process specified witness computes
- part of each commitment R, the demonstrator sends the controller all or

. Step 2: act of challenge d

part of each commitment R, produces challenges d whose number is equal to the number of commitments R and sends the challenges d to the demonstrator, the controller, after having received all or

. Step 3: act of response D

according to claim 1, challenges d by - the witness computes the responses D applying the process specified from the

. Step 4: act of checking

controller, the demonstrator sends each response D to the

computes controller, having the m public values G1, G2 ..., Gm, challenge transmitted a part commitment R' satisfying a relationship of the type: each commitment case where the demonstrator has transmitted a part מ d and each response D, this reconstructed reconstructed commitment R', from of each commitment R, **R** if the demonstrator the

 $R' \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^V \mod n$

or a relationship of the type

$$\mathbf{R'} \equiv \mathbf{D'}/\mathbf{G_1}^{\mathbf{d1}}.\mathbf{G_2}^{\mathbf{d2}}.\dots \mathbf{G_m}^{\mathbf{dm}}. \mod \mathbf{n}$$

commitment R' reproduces all or part of each commitment R that has been transmitted to it, the controller ascertains that each reconstructed

totality of each commitment R where the demonstrator has transmitted the

commitment R satisfies a relationship of the type each commitment R, the controller, having the if the demonstrator has transmitted the totality values G1, G2,... Gm, ascertains that

 $R' \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^V \mod n$

or a relationship of the type

 $R' \equiv D^{v}/G_1^{d1}.G_2^{d2}...G_m^{dm}. \mod n_{\underline{\cdot}}$

Claims 3 and 4 are not changed.

prove the authenticity of the message M by checking the 5. (Amended) Method according to claim 4, designed to Checking operation signed message through an entity called a controller;

message executes a checking operation by proceeding as follows: the said controller entity having the signed

challenges d, responses D, case where the controller has commitments ₽,

responses D, if the controller has commitments R, challenges d,

relationships of the type the challenges d and the responses the controller ascertains that the commitments U satisfy

 $R \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^V \mod n$

or relationships of the type

 $R \equiv D^{V}/G_1^{d1}.G_2^{d2}....G_m^{dm}. \mod n$

hashing function challenges d and the commitments the controller ascertains that the message M, R satisfy the

d = h (message, R)

and responses D case where the controller has challenges d

Į. the controller has challenges Ω and

responses D, each challenge d and response D, commitments the controller reconstructs, on the basis of

 $R' \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^V \mod n$

satisfying relationships of the type:

or relationships of the type

and the challenges d satisfy the hashing function the controller ascertains that the message ${\tt M}$

. case where the controller has commitments R and d=h(message,R')

responses D

if the controller has commitments R and responses D,

and reconstructs d' the controller applies the hashing function

d' = h (message, R)

R, the challenges d' and the responses D relationships of the type: the controller ascertains that the commitments satisfy

 $\mathbf{R} \ \equiv \ \mathbf{G_1}^{\mathbf{d1}}.\mathbf{G_2}^{\mathbf{d2}}. \ ... \ \mathbf{G_m}^{\mathbf{dm}}. \ \mathbf{D^V} \ \mathbf{mod} \ \mathbf{n}$

or relationships of the type

 $R \equiv D^{V}/G_1^{d1}.G_2^{d2}....G_m^{dm}. \mod n$

controller server, 6. (Amended) System designed t O prove, t O

- the authenticity of an entity and/or
- this entity, the integrity of a message M associated with

parameters or derivatives of these parameters: by means of all or part of the following

- public values $G_1,G_2,\ \ldots \ G_m$ (m being greater than or equal to 1), m pairs of private values Q1, Q_2 , ...
- equal to 2), f prime factors p_1 , p_2 , ... p_f (f being greater than or a public modulus n constituted by the product of

values being related by relations of the following the said modulus and the said private and public

 $G_{\underline{i}} \cdot Q_{\underline{i}}^{\ \ v} \equiv 1 \cdot \text{mod } n \text{ or } G_{\underline{i}} \equiv Q_{\underline{i}}^{\ \ v} \text{ mod } n;$

where v denotes a public exponent of the form:

$$v = 2^k$$

where k is a security parameter greater than 1;

prime factors p1, p2, ... pf; distinct base numbers $g_1,\ g_2,\ ...\ g_m,\$ smaller than the f said m public values Gi being squares gi

said m base numbers g1, g2, ... gm being produced such that the following conditions are satisfied: the said p1, p2, ... pf prime factors and/or the

First condition

each of the equations:

 $x_{v^{\underline{\vee}}} \equiv g_{\underline{1}}^2 \mod n \pmod{1}$

modulo n; can be resolved in x in the ring of integers

Second condition

by taking Qi squared modulo n, k-1 times, one of them is not equal to $\pm g_i$ (in other words is not trivial) $\pm c_i$ if $G_i \equiv Q_i^V \mod n$, among the m numbers q_i obtained

obtained by taking the inverse of Qi modulo n squared modulo n, k-1 times, one of them is not equal to $\pm 9i$ (in other words is not trivial); if $G_{\dot{1}}.Q_{\dot{1}}^{V} \equiv 1 \mod n$, among the m numbers $q_{\dot{1}}$

Third condition

at least one of the 2m equations

$$x^2 \equiv g_1 \mod n + (2)$$

$$x^2 \equiv -g_{imod n} + \frac{3}{3}$$

can be resolved in x in the ring of integers

modulo n;

example, takes the form of a microprocessor-based bank contained especially in a nomad object which, the said system comprises a witness device,

the witness device comprises

and/or the m numbers of bases gi and/or parameters of private values Q_i and of the public exponent v_i public modulus n and/or the m private values $Q_{
m i}$ and/or the Chinese remainders of the prime factors and/or the the said witness device also comprises: the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_{i} \mod p_{j}$) of the a memory zone containing the f prime factors

- device, called random value production means of the witness random value production means, hereinafter
- n; each commitment being computed: to compute commitments R in the ring of integers modulo computation of commitments R of the witness device, computation means, hereinafter called means
- either by performing operations of the type:

$$R_i \equiv r^V \mod n$$

value production means, and r is such that 0 < r < n; is a random value produced by the random

or by performing operations of the type:

$$R_i = r_i^{V} \mod p_i$$

prime number p_i such that $0 < r_i < p_i$ each r_i belonging applying the Chinese remainders method; produced by random value production means, then by a collection of random values {r1, r2,... rf} where ri is a random value associated with

the said witness device also comprises:

- challenge d comprising m integers di hereinafter called elementary challenges; device, to receive one reception of the challenges d of the - reception means hereinafter called the means for or more challenges d; each witness
- challenge d, of a response D, device for the computation of the computation means, hereinafter called means for computation, on the basis of each responses D of the witness
- either by performing operations of the type:

 $D \equiv r.Q1^{d1}.Q2^{d2}. \dots Qm^{dm} \mod n$

. or by performing operations of the type:

 $D = r.Qi, 1^{d1}.Qi, 2^{d2}. ... Qi, m^{dm} mod pi$

method-, and then by applying the Chinese remainders

as there are commitments R, each group of numbers R, d, there are as many responses D as there are challenges d commitments R and one or more responses D; transmission means to transmit one or more

D forming a triplet referenced {R,d,D}.

demonstrator and an entity called a controller, 7. (Amended) the said system being such that it comprises: the authenticity of an entity called System according to claim 6, designed

demonstrator entity, the said demonstrator device being microprocessor-based bank card, especially of logic microcircuits in a nomad object, interconnection means interconnected example the form of a microprocessor in a - a demonstrator device associated with the with and possibly taking the the witness device

connection means for its electrical, electromagnetic, especially taking the form of a data-processing optical or acoustic connection, controller demonstrator device; the said controller entity, the said communications controller device associated with the especially through a device network, terminal or remote controller device comprising

following steps: the said system enabling the execution of the

. Step 1: act of commitment R

commitment R by applying the process commitments R of the witness device compute each according to claim 1, each call, the means of computation

witness device, to transmit all or part of each interconnection means, commitment R to the demonstrator device through the hereinafter called the the witness device has means of transmission, transmission means 0 f

commitment R to the controller device through the demonstrator device, to transmit all or part of each means, hereinafter called the transmission means of the connection means; demonstrator device also has transmission

Step 2: act of challenge d

equal in number to the number of commitments R, all or part of each commitment R, of the challenges d production means for the production, after receiving controller device comprises challenge

demonstrator through connection means, controller, hereinafter the controller device also has transmission means, to transmit denoted transmission means challenges 0 H

Step 3: act of response D

demonstrator device through the interconnection means, witness device receive each challenge d coming from the the means of reception of the challenges d of the

challenges d by witness device compute the according to claim 1, the means of computation of the responses D of the applying the process responses D specified from the

Step 4: act of checking

each response D to the controller, transmission means of the demonstrator transmit

the controller device also comprises:

- computation means of the controller device, computation means, hereinafter called the
- comparison means of the controller device, comparison means, hereinafter called the

each commitment R where the demonstrator has transmitted a part of

relationship of the type: D, this reconstructed commitment R' satisfying commitment R', from each challenge d and each response public values G_1 , G_2 , ..., G_m , compute a reconstructed computation means of the controller device, having m transmitted if the transmission means of the demonstrator have a part of each commitment

 $R' \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^V \mod n$

or a relationship of the type

 $\texttt{R'} \equiv \texttt{D''}/\texttt{G1}^{\texttt{d1}}.\texttt{G2}^{\texttt{d2}}. \dots \texttt{Gm}^{\texttt{dm}}. \text{ mod } \texttt{n}$

part of each commitment R received, compare each reconstructed commitment R' with all or comparison means of the controller device

totality of each commitment R case where the controller has transmitted

controller device, having m public values G1, G2, ..., computation means and the comparison means of the transmitted the totality of each commitment relationship of the type ascertain that each commitment R satisfies transmission means of the demonstrator have R, the

 $\texttt{R} \equiv \texttt{G1}^{\texttt{d1}}.\texttt{G2}^{\texttt{d2}}. \ ... \ \texttt{Gm}^{\texttt{dm}}. \ \texttt{D}^{\texttt{V}} \ \texttt{mod} \ \texttt{n}$

or a relationship of the type

 $R \equiv D^{V}/G_1^{dl}.G_2^{d2}....G_m^{dm}. \mod n$

the integrity of a message M associated with an entity 8. (Amended) known as a demonstrator, give proof to an entity known as a controller, System according leto claim 6, designed

the said system being such that it comprises

demonstrator entity, the said demonstrator device being microprocessor-based bank card, especially of logic microcircuits in a nomad object, interconnection means and possibly taking the form interconnected example the form of a microprocessor demonstrator device associated with with the witness device in a

optical or acoustic connection, especially through a server, the said controller device comprising especially taking the form of a connection means for its electrical, electromagnetic, demonstrator device; controller processing controller device entity, communications the said associated with the terminal or remote controller device network,

following steps: the said system enabling the execution of the

. Step 1: act of commitment R

according to claim 1, commitment R by applying the process commitments R of the witness device at each call, the means of computation compute each

witness device, to transmit all or part of each commitment R to the demonstrator device through the hereinafter called the transmission interconnection means, witness device has transmission means of the

Step 2: act of challenge d

demonstrator, applying a hashing function h whose means, hereinafter called the computation means of the commitment R to compute at least one token T, arguments the demonstrator device comprises computation are the message M and all or part of each

means, hereinafter known as the transmission means token T, of the challenges d in a number equal to means for the production, after having received through the connection means to the controller device, number of commitments R, controller device also has challenge production demonstrator the demonstrator device also has transmission device, to transmit each

demonstrator through the connection means; controller, hereinafter the controller device also has transmission means, to transmit the called the transmission means challenges d 0 fi t 0 the

Step 3: act of response D

demonstrator device through the interconnection means, witness device receive each challenge d coming from the the means of reception of the challenges d of the

challenges d by applying according to claim 1, the means of computation of the responses D of the device compute the the responses process U specified

. Step 4: act of checking

transmit each response D to the controller, the transmission means of the demonstrator

means, hereinafter called the computation means of the commitment R', from each challenge d and each response controller relationship of the type: this reconstructed commitment R' satisfying in order the controller device also comprises computation device, having m public values G1, G2,..., to firstly compute a reconstructed

 $R' \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^V \mod n$

or a relationship of the type

 $\mathbf{R'} \equiv \mathbf{D'}/\mathbf{G_1}^{\mathrm{dl}}.\mathbf{G_2}^{\mathrm{d2}}....\mathbf{G_m}^{\mathrm{dm}}. \ \mathrm{mod}\ \mathbf{n}$

and all or part or each reconstructed commitment R', hashing function h having as arguments the message M secondly, compute a token T' by applying the

received token T. controller device, to compare the token T' with the hereinafter the controller device also has comparison means, known S the comparison means of

Claim 9 is not changed.

10. (Amended) System according to claim 9, designed to signed message by means of an entity called the prove the authenticity of the message M by checking the controller;

Checking operation

controller device comprising connection means for its entity, the said controller device especially taking the form of a terminal or remote server, the said controller device associated with the controller communications network, to the signing device; connection, especially through a electrical, the said system being such that it comprises electromagnetic, optical or acoustic data-processing

means, in such a way that the controller device has a signing device, for the transmission, to the controller hereinafter known as the transmission means of signed message comprising: of the signed message through the connection said signing device associated with the entity comprises transmission

- the message M,
- the challenges d and/or the commitments R,
- the responses D;

the controller device comprises:

- computation means of the controller device, computation means hereinafter the
- comparison means of the controller device-: comparison means, hereinafter called the
- challenges d, responses D case where the controller device has commitments

responses D, if the controller has commitments R, challenges d,

challenges d and the responses D satisfy relationships controller device ascertain that the commitments R, of the type . . the computation and comparison means of the

$$R \equiv G_1^{d1}.G_2^{d2}....G_m^{dm}.D^V \mod n$$

or a relationship of the type

$$R \equiv D^{v}/G_1^{d1}.G_2^{d2}....G_m^{dm}. \mod n$$

controller device challenges d and the commitments R satisfy the hashing . . the computation and comparison means ascertain that the message of the

d = h (message, R)

d and responses D . case where the controller device has challenges

responses D, if the controller device has challenges d and

device, on the basis of each challenge relationships of the type: response . the D, compute commitments computation means of the d and each controller satisfying

$$R \equiv G_1^{d1}.G_2^{d2}. \dots G_m^{dm}. D^V \text{ mod } n$$

or a relationship of the type

$$R \equiv D^{v}/G_1^{dl}.G_2^{d2}....G_m^{dm}. mod n$$

challenges d satisfy the hashing function: controller device ascertain that the message M and the the computation and comparison means of

$$d = h \text{ (message, R')}$$

responses D case where the controller device has commitments R

if the controller device has commitments R and

apply the hashing function and compute d' such that the computation means of the controller device

d' = h (message, R)

of the type: challenges d' and the responses D satisfy relationships controller device ascertain that the commitments R, the . the computation and comparison means of the

 $\mathbf{R} \ \equiv \ \mathbf{G_1}^{\mathbf{d1}}.\mathbf{G_2}^{\mathbf{d2}}. \ ... \ \mathbf{G_m}^{\mathbf{dm}}. \ \mathbf{D^V} \ \mathbf{mod} \ \mathbf{n}$

or a relationship of the type

 $R \equiv D^{v}/G_1^{dl}.G_2^{d2}....G_m^{dm}. \mod n_{\underline{\cdot}}$

microprocessor-based bank card, designed to prove to a 11. (Amended) Terminal device associated with controller device: entity, taking the form especially of a nomad object, example the form of a microprocessor

- the authenticity of an entity and/or

the integrity of a message M associated with

parameters or derivatives of these parameters: by means of all or part of the following

values $G_1,G_2,\ \ldots \ G_m$ (m being greater than or equal to 1), m pairs of private values $Q_1,\ Q_2,\ \dots\ Q_m$ and public

equal to 2), prime factors p_1 , p_2 , ... p_f (f being greater than or a public modulus n constituted by the product

values being related by relations of the following type the said modulus and the said private and public

where v denotes a public exponent of the form:

 $\text{Gi.Q}_{i}^{\text{V}} \equiv 1 \mod n \text{ or Gi} \equiv \text{Q}_{i}^{\text{V}} \mod n;$

where k is a security parameter greater than 1:

distinct base numbers g1, g2, ... gm, smaller than the prime factors p1, p2, ... pf÷<u>;</u> the said m public values $G_{
m i}$ being squares ${g_{
m i}}^2$ of m

said m base numbers g1, g2, ... gm being produced such that the following conditions are satisfied: the said p1, p2, ... pf prime factors and/or the

First condition

each of the equations:

$$x_{y}^{\vee} \equiv g_{\dot{1}}^{2} \mod n - (1)$$

can be resolved in x in the ring of integers

Second condition

is not equal to ${}^{\pm}g_i$ (in other words is not trivial), by taking Qi if $G_{i} \cdot Q_{i}^{V} \equiv 1 \mod n$, among the m numbers q_{i} obtained by times, one of them is not equal to +gi (in other words taking the inverse of Q_1 modulo n squared modulo n, k-1if $Gi \equiv Q_i^V \mod n$, among the m numbers q_i obtained squared modulo n, k-1 times, one of them

Third condition

is not trivial);

at least one of the 2m equations

$$x^2 \equiv g_{i} \mod n - (2)$$

 $x^2 \equiv -g_{imod} n - (3)$

can be resolved in x in the ring of integers

modulo n-; the said terminal device comprises a witness

and/or the m numbers of bases g_i and/or parameters device comprising a memory zone containing the f prime factors

public modulus n and/or the m private values $Q_{
m i}$ and/or private values Q_i and of the public exponent v_i the f.m components $Q_{i,j}$ ($Q_{i,j} \equiv Q_{i} \mod p_{j}$) of the the Chinese remainders of the prime factors and/or the

the said witness device also comprises:

- called random value production means of the witness random value production means, hereinafter
- the computation of commitments R of the witness device, n; each commitment being computed: to compute commitments R in the ring of integers modulo computation means, hereinafter called means for
- either by performing operations of the

 $R \equiv r^{V} \mod n$

value production means, and r is such that 0 < r < n. where r is a random value produced by the random

or by performing operations of the type:

Ri = ri mod pi

prime number p_i such that $0 < r_i < p_i$ each r_i belonging a collection of random values $\{r_1, r_2, \dots r_f\}$ where ri is a random value associated with the

applying the Chinese remainders method; produced by random value production means, then by

the said witness device also comprises:

- device, to receive one or more challenges d; each challenge d comprising m integers di hereinafter called elementary challenges; reception of the challenges - reception means hereinafter called the means for d of the witness
- device for the computation of the challenge d, of a response D, computation means, hereinafter called means for the computation, on the basis of each responses D of the witness
- . either by performing operations of the type:

 $D \equiv \text{r.Q1}^{\text{d1}} \cdot \text{Q2}^{\text{d2}} \cdot \dots \cdot \text{Qm}^{\text{dm}} \text{ mod } n$

. or by performing operations of the type:

 $D \equiv r.Q_{i,1}^{d1}.Q_{i,2}^{d2}...Q_{i,m}^{dm} \mod p_{i}$

then by applying the Chinese remainders

as there are commitments R, each group of numbers R, d, there are as many responses D as there are challenges d commitments R and one or more responses D; D forming a triplet referenced {R, d, D}. transmission means to transmit one or more

Claims 12-14 are not changed.

- controller entity, designed to prove: form of a terminal or remote server associated with a (Amended) Controller device especially taking
- the authenticity or an entity and/or

this entity. the integrity of a message M associated with

parameters or derivatives of these parameters: by means of all or part of the following

greater than or equal to 1), m pairs of public values $G_1, G_2, \ \ldots \ G_m$ (m being

associated controller entity, equal to 2), unknown to the controller device and the prime factors p_1 , p_2 , ... p_f (f being greater than or a public modulus n constituted by the product of

values being related by relations of the following type the said modulus and the said private and public

 G_i . $Q_i^{V} \equiv 1$. mod n or $G_i \equiv Q_i^{V}$ mod n;

where v denotes a public exponent of the form:

k is a security parameter greater than 1;

controller device, associated with the public value Gi; Qi is a private value, unknown († 0 the

distinct base numbers g_1 , g_2 , ... g_m , smaller than the fprime factors p1, p2, ... pf; the said m public values ${ t G_i}$ being squares ${ t g_i}^2$

that the following conditions are satisfied: m base numbers g1, g2, ... gm being produced such said p1, p2, ... pf prime factors and/or the

First condition

each of the equations:

 $x_{\psi}^{\vee} \equiv g_1^2 \mod n + (1)$

modulo n can 0 resolved in x in the ring of integers

Second condition

by taking Qi squared modulo n, k-1 times, one if $G_{i} \cdot Q_{i}^{V} \equiv 1 \mod n$, among the m numbers q_{i} obtained by is not equal to ${}^{\pm}g_1$ (in other words is not trivial)-. taking the inverse of Q_1 modulo n squared modulo n, k-1 if $Gi = Q_i^V \mod n$, among the m numbers q_i obtained of them

times, one of them is not equal to +gi (in other words

Third condition

is not trivial);

at least one of the 2m equations

$$x^2 \equiv g_{i} \mod n + (2)$$

$$x^2 \equiv -g_{imod n}$$
 (3)

modulo n. can be resolved in x in the ring of

designed to prove the authenticity of an entity called 16. (Amended) Controller device according to claim 15, demonstrator to an entity called a controller;

acoustic connection, especially through a datameans for its device associated with the demonstrator entity; processing communications network, to the said controller device comprising connection electrical, electromagnetic, optical or a demonstrator

the following steps: said controller device being used to execute

challenge d Steps 1 and 2; act of commitment R, act of

reception of all or part of said controller device the commitments also has means R coming for

from the demonstrator device through the connection

means for the production, after receiving all or part equal to the number of commitments R, each challenge challenges-, comprising m integers di hereinafter called elementary each commitment R, the controller device has challenge of the challenges d in a number production

controller, to transmit the hereinafter demonstrator through the connection means; the controller device also has transmission means, called transmission means challenges d to Of the the

- the said controller device also comprises: Steps 3 and 4: act of response, act of checking
- connection means, coming means for the reception of the from the demonstrator device, responses D through the
- computation means of the controller device, computation means, hereinafter the
- comparison means of the controller device, comparison means, hereinafter called the

each commitment R. case where the demonstrator has transmitted a part

 G_1 , G_2 , ..., G_m compute a reconstructed commitment $R^{\,\prime}$, means or the controller device, having m public values received a part of each commitment R, the computation reconstructed commitment R' satisfying a relationship of the type: if the reception means of the demonstrator have each challenge d and each response D, this

 $\texttt{R'} \equiv \texttt{G1}^{\texttt{d1}}.\texttt{G2}^{\texttt{d2}}. \; ... \; \texttt{Gm}^{\texttt{dm}}. \; \texttt{D^V} \; \texttt{mod} \; \texttt{n}$

or a relationship of the type

 $R' \equiv D^{\text{v}}/G_1^{\text{dl}}.G_2^{\text{d2}}....G_m^{\text{dm}}. \text{ mod } n$

part of each commitment R received, compare each comparison means of the controller reconstructed commitment R' with all or device

totality of each commitment R case where the demonstrator has transmitted the

relationship of the type: controller device, having m public values G1, G2, ..., computation means and the comparison means of have received the totality of each commitment R, the ascertain that each commitment R satisfies if the reception means of the controller device

or a relationship of the type

 $R \equiv D^{v}/G_1^{d1}.G_2^{d2}....G_m^{dm}. \mod n$

Claim 17 is not changed.

designed to prove the authenticity of the message M by 18. (Amended) Controller device according to claim 15, a signed message; checking a signed message by means of an entity called

associated with a signing entity function h (message, R), comprising: signed message sent by having a hashing Ŋ signing device

- the message M,
- the challenges d and/or the commitments R
- the response D;

Checking operation

means for its electrical, electromagnetic, optical or signing device, through the connection means, device having received the signed message associated with the signing entity, the said controller processing communications network, to a signing device acoustic the said controller device comprising connection connection, especially through a

the controller device comprises:

- computation means of the controller device, computation means, hereinafter called the
- comparison means of the controller device; comparison means, hereinafter called the
- case where the controller device has commitments

R, challenges d, responses D if the controller has commitments R, challenges d,

relationships of the type the controller device ascertain that the commitments challenges d and the responses D . the computation and comparison means of satisfy

 $R \equiv G_1^{d_1}.G_2^{d_2}....G_m^{dm}.D^v \mod n$

or a relationship of the type

 $R \equiv D^{v}/G_1^{d1}.G_2^{d2}....G_m^{dm}. \mod n$

challenges d satisfy the hashing function controller device ascertain that the message M and the . the computation and comparison means of the

d = h (message, R)

R and responses D case where the controller device has commitments

responses D-, if the controller device has commitments R and

apply the hashing function and compute d' such that . the computation means of the controller device

d' = h (message, R')

of the type: challenges d' and the responses D satisfy relationships controller device ascertain that the commitments R, the . the computation and comparison means of the

 $R = G1^{d1}.G2^{d2}. ... Gm^{dm}. D^V mod n$

or a relationship of the type

 $R \equiv D^{v}/G_1^{d1}.G_2^{d2}...G_m^{dm}. \mod n_{\underline{\cdot}}$

apy

METHOD, SYSTEM, DEVICE FOR PROVING THE AUTHENTICITY OF AN ENTITY OR THE INTEGRITY OF A MESSAGE

The present invention relates to the methods,

and/or the integrity and/or authenticity of a message.

and devices designed to prove the authenticity of an entity

shall be used to describe the present invention. expression "GQ2", or "GQ2 invention" or "GQ2 technology" the terms method. Hereinafter, reference shall be made to their work by Guillou The patent EP 0 311 470 B1, whose inventors are Louis and "GQ patent" Jean-Jacques Quisquater, or "GQ method". describes Hereinafter, such

S

10 15 20 "witness" that he knows the RSA signature of his identity without is my identity; I know its RSA signature". The witness signature. Thereafter, the witness declares the following: "Here process, the trusted authority gives the witness an identity and "trusted authority" assigns an identity to each entity called a that the RSA signature distributed by the trusted authority, an knowledge". The mechanisms using the GQ method run "without transfer "controller" According and computes it. Through the According ascertains, to the GQ method, to the GQ method, the witness does not without obtaining corresponds to the declared identity its RSA signature. In a customizing RSA public identification an entity known as knowledge entity known as a thereof, proves

know a large number of identities. the RSA private key with which the trusted authority

on the factorization of the modulus n, this dependence is called "multiplicative attacks" against the various standards an equivalence, indeed far from it, as can be seen in what are technology. However, digital signatures implementing RSA technology. The GQ technology described above makes use of RSA whereas RSA technology truly depends of

Ø

70 20 15 n. Any attack on the triplets GQ2 leads to factorization of the is equivalent to knowledge of the factorization of the modulus inherent in RSA technology. Knowledge of the GQ2 private drawbacks of RSA technology. self-authenticating entity and for technology, the work load is reduced both for the signing or modulus n: this time there is equivalence. With the both security and performance, the GQ2 technology averts the Through a better use of the problem of factorizing technology to The improve the performance goal of the GQ2 technology and, on the other hand, the controller is twofold: on the to avert the characteristics in terms problems of entity. one o f

infrastructures, numbers comprising 512 bits or more. These computations in seeking to cards to pay for their purchases. It may be recalled here multiple arithmetical applications involved in methods arithmetical coprocessors. of monolithic powers of the order of $2^{16}+1$. But existing relate to numbers having substantially the same size raised to questions the GQ method leads to computation times which, in certain difficult The GQ method implements modulo computations prove to be disadvantageous for consumers using authorities to solve. have especially in the field of bank cards, make self-programmable increase to be examined: on the have raised a problem that is n the fact, two The security work microprocessors apparently of payment load one hand, microelectronic related contradictory particularly increasing cards, such as without to that bank

25

30

35

security by using increasingly lengthy and distinct keys This problem becomes especially acute the necessary existing microprocessor components. card while, leading to excessive computation to take account of the existing infrastructure on the other hand, preventing inasmuch as it is times for the users. the work load

problem while still increasing security. The GQ2 technology is aimed at providing a solution to

Ŋ

designed to prove the following to a controller entity: More particularly, the invention relates to a method

the authenticity of an entity and/or

following parameters or derivatives of these parameters: proof - the integrity of a message M associated with this entity. 1Sestablished by means of all or part of the

 G_{1} G₂, ... G_m (m being greater than or equal to 1), - m pairs of private values Q₁, Q₂, ... Q_m and public values

prime Said modulus and said private and public factors $p_1, p_2, ..., p_f$ (f being greater than or equal to a public modulus constituted product values 2).

ם

by the

of f

20

25

15

related by relationships of the $G_i \cdot Q_i^{\ \nu} \equiv 1 \cdot \text{mod } n \text{ or } G_i \equiv$ type: Qi mod n

where v represents a public exponent of the type $v = 2^k$

numbers said m public values G_i being the squares g_i^2 of m distinct base $p_1, p_2, \dots p_f;$ where k g₁ g₂, ... g_m inferior said f prime factors p₁, p₂,...p_f and/or is a security parameter greater than 1, to the f prime said factors

First condition

30

the

following conditions

base numbers

g₁ g₂, ... g_m being produced

in such a way that

are satisfied.

According to the first condition, each of the equations $x^{v} \equiv g_{i}^{2}$ mod n \bigcirc

has solutions in x in the ring of integers modulo

Second

35

different from ±g_i (that is to say non-trivial). Q_i to the square modulo n, k-1 rank times, $G_i \equiv Q_i^{\text{v}} \mod n$, among the m numbers According to the second condition, qi obtained by raising in the one of them is case where

non-trivial). rank times, one of them is different from ±gi (that is to say raising the inverse of Qi modulo n to the square $G_i \cdot Q_i^{\vee} \equiv 1 \text{.mod } n,$ According to the second condition, in among the m numbers the case where q_i obtained modulo n, k-1 ЬV

±gi represents the number It is to be noted here that according gi and n-gi. to current notation

Third condition

10

S

equations: According ō the third condition, among the 2 m

$$\mathbf{x}^2 \equiv \mathbf{g_i} \mod \mathbf{n} \quad (2)$$

15

x² ≡ -gi mod n (3)

integers modulo n. at least one of them has solutions in x in the ring o f

20 steps the components $Q_{i,j}(Q_{i,j} \equiv Q_i \mod p_j)$ of the private values Q_i and of factors p_i and/or m Chinese remainders public exponent v. defined here The method implements an entity called a witness in the ב and/or the m private base numbers of the prime below. Said witness entity has f prime gi and/or parameters values Qi and/or the f.m factors and/or the public of the

integers modulo n. The witness computes commitments Each commitment is computed either by: R in the ring

performing operations of the type

 $R \equiv r^{v} \mod n$

a random value such that 0<r<n,

o r

30

Where

r is

25

by performing operations of the type $R_i \equiv r_i^{\ \ \ } \mod p_i$

collection of random values $\{r_1, r_2, ..., r_f\}$, number where p_i such that $0 < r_i < p_i$, each r_i Γ_i is a random value associated belonging with the prime 6 9

** then by applying the Chinese remainder method

challenge challenge elementary The d_i computes a response D, witness receives one or more d comprises challenges. The witness, m integers di on challenges the hereinafter basis ofd. called each Each

- either by performing operations of the type: $D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot ... \cdot Q_m^{dm} \mod n$

-

10

S

** by performing operations of the type: $D_i \equiv r_i \cdot Q_{i,1}^{d1}, \ Q_{i2}^{d2} \cdot ... \cdot Q_{i,m}^{dm} \ mod \ p_i$

** then by applying the Chinese remainder method.

group of numbers R, d, D forms a triplet referenced {R, d, D}. as there The method is such that there are challenges d as there are are as many responses D commitments

15

Case of the proof of the authenticity of an entity

20 authenticity of an entity known as a demonstrator to an entity according the known as the controller. following steps: witness. Said demonstrator In a first variant of to the invention is Said demonstrator entity comprises an embodiment, and controller designed to entities the method prove execute the

Step 1: act of commitment R

25

sends the controller all or part of each commitment R. applying the process specified above. The demonstrator At each call, the witness computes each commitment

• Step 2: act of challenge d

30

number of commitments commitment R, produces demonstrator. The controller, after having received all or part of each challenges d equal in number to the R and sends the challenges d to the

Step 3: act of response D

challenges d by applying The witness computes the process the specified above. responses U from the

• Step 4: act of checking

S

controller. The demonstrator sends each response Ū ō the

each First case commitment R. : the demonstrator has transmitted a part of

commitment R, the controller, having commitment R' satisfying a relationship of the type G₂, ..., G_m, computes a reconstructed each challenge d and each response If the demonstrator has transmitted $R' \equiv G_1^{dl} \cdot G_2^{d2} \cdot ... \cdot G_m^{dm} \cdot D^v$ the m public commitment D, this mod n a part of reconstructed values G₁, R', from each

10

a

15

relationship of the type $R' \equiv D^{v}/G_1^{d1} \cdot G_2^{d2} \cdot ... G_m^{dm} \cdot mod n.$

commitment R' reproduces all or part of each commitment R that has been transmitted to it. The controller ascertains that each reconstructed

totality Second of each commitment R case : the demonstrator has transmitted the

20

commitment R, the controller, having the relationship of the type If the demonstrator G_m, ascertains that each commitment R satisfies has transmitted the totality of each m public values

 $R \equiv G_1^{dl}$. G_2^{d2} $.\,\,...\,\,G_m{}^{dm}\,\,.\,\,D^{v}$ mod n

25

or a relationship of the type $R \equiv D^{v}/G_1^{dl} \cdot G_2^{d2} \cdot \cdot$

. ... G_m dm mod n.

Case of the proof of the integrity of the message

demonstrator entity comprises the associated invention is designed to provide combined controller In a second variant of an embodiment capable of being with an entity called a demonstrator with the entity, of first one, the method according to the the proof to an entity, known integrity witness. of entity. Said as

30

following Said demonstrator steps: and controller entities perform the

Step 1: act of commitment R

bу applying the At each call, the witness computes process specified above. each commitment ∇

• Step 2: act of challenge

S

and sends the challenges d to the demonstrator. demonstrator challenges controller, arguments commitment The demonstrator applies d equal in number to the number of commitments R are after having received π sends the the to message compute token T to M and all at a hashing least ы token the one or function controller. token part produces h whose \mathbf{of} Τ. each The

0

Step 3: act of response J

15

challenges d by applying the process specified above. The witness computes the responses U from the

Step 4: act of checking

controller. The controller, having the m public values G1, G2, ... commitment R' challenge computes The demonstrator a $R' \equiv G_1^{dl} \cdot G_2^{d2} \cdot \dots G_m^{dm} \cdot D^v \mod n$ and a reconstructed commitment satisfying a relationship of the type: each sends response each Ų, response this R', from reconstructed U each the

20

 $^{\circ}$

25

a relationship of the type $R' \equiv D^{v}/G_1^{dl} \cdot G_2^{d2} \cdot \cdot$ G_m dm . mod n.

Then the controller ascertains that the token T' is identical arguments reconstructed commitment token Then T transmitted. the controller applies the hashing function h whose are the message R' to reconstruct M and all or part the token ofeach t o

authenticity signature of þ message and proof \mathbf{of} its

invention, capable of being embodiments, In a third variant of the method an embodiment combined with the two preceding according to according the invention Ç the

35

30

the witness. entity known as the signing entity. Said signing entity designed to produce the digital signature of a message includes M by an

Signing operation

S

Ö obtain a signed message comprising: Said signing entity executes a signing operation in order

- the message M,
- the challenges d and/or the commitments

7,

the responses D.

10

implementing the following steps: Said signing entity executes the signing operation ЬУ

• Step 1: act of commitment R

bу applying the process specified above. At each call, the witness computes each commitment ∇

• Step 2: act of challenge 2

15

obtain a binary train. arguments commitments extracts challenges d in a number equal to the number of The signing are **7**2. the message M and each entity applies From this binary train, the signing a hashing commitment function h whose entity Rto

Step 3: act of response D

20

Checking challenges The witness computes d by applying the process specified process above. operation the responses U from the

operation by entity called To prove a controller checks the signed message. Said controller having proceeding as follows, the the authenticity of the signed message carries out message M, an entity ย checking

25

Case where the controller has commitments ₹,

responses D, the challenges challenges type: the controller has commitments d and the responses controller ascertains that the D satisfy relationships Р, commitments challenges d, ₹,

 π G_1^{dl} . G_2^{d2} $.\,\,...\,\,G_m{}^{dm}\,\,.\,\,D^v$ mod n

35

30

d,

responses

J

or relationships of the type: $\frac{D}{dt} = \frac{D^{3}}{dt} = \frac{d^{2}}{dt}$

 $R \equiv D^{v}/G_1^{dl} \cdot G_2^{\tilde{d2}} \cdot \dots \cdot G_m^{dm} \cdot \text{mod } n.$

challenges function: the controller ascertains that the message <u>a</u> and the commitments \mathbb{R} satisfy the hashing M, the

d = h (message, R)

S

responses Case where U the controller has challenges ٥ a n d

10 controller, on the basis type: D, reconstructs commitments R' satisfying relationships If the controller has challenges of each challenge d and responses d and each response D, the of the

 $R' \equiv G_1^{dl} \cdot G_2^{d2} \cdot \dots G_m^{dm} \cdot D^v \mod n$

or relationships of the type:

15

 $R' \equiv D^{v}/G_1^{dl} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot mod n.$

the challenges d satisfy the hashing function: Then the controller ascertains that the message M and

D = h (message, R')

and responses Case where U the controller has commitments π

20

the controller applies the hashing function and reconstructs If the controller has commitments **d**' = h (message, R). R and responses D, ď

25 the the challenges d' and the responses type: Then the controller ascertains that the commitments D satisfy relationships οf ₹,

 $R \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot \dots G_m^{d'm} \cdot D^v \mod n$

or relationships of the type:

 $R \equiv D^{v}/G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \cdot \mod n$

30 System

ō prove the following to a controller server: The present invention also relates to a system designed

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity.

following This proof is established by means of all or part of the parameters or derivatives of these parameters:

G₁, G₂, ... G_m (m being greater than or equal to 1), pairs of private values Q1, Q2, ... Qm and public values

prime factors $p_1, p_2, ..., p_f$ (f being greater than or equal to a public modulus n constituted by the product of f

S

linked by relationships of the type: Said modulus, and said private and public values

 $G_i \cdot Q_i^{v} \equiv 1 \cdot \text{mod } n \text{ or } G_i \equiv Q_i^{v} \text{ mod } n$

v designating a public exponent of the type:

10

 $v=2^k$

conditions are satisfied. numbers g₁, g₂ ... g_m being produced such that the following ... p_f; said f prime factors p₁, p₂, ... p_f and /or said m base base numbers said m public values Gi being the squares g_i^2 of distinct m where k is a security parameter greater than I, g₁, g₂, ... g_m inferior to the f prime factors p₁, p₂,

15

First condition

20

According to the first condition, each of the equations: $x^{v} \equiv g_{i}^{2}$. mod n (1)

can be solved in x in the ring of integers modulo n

Second condition

 $G_i \equiv Q_i^{\ \nu}$, mod n, among the m numbers q_i obtained by raising different from ± Qi to the square modulo n, k-1 rank times, According to the second condition, gi (that is to say non trivial). in the case one of them is where

25

30

raising the inverse of Q_i modulo n to the square modulo n, k-1 $G_i \cdot Q_i^{V} \equiv 1 \mod n$, among the m numbers non trivial). rank times, one of them is different from $\pm g_i$ (that is to say According to the second condition, in the q_i obtained case where ЬУ

Third condition: $notation \pm$ is pointed gi represents the numbers out here that gi and n-gi. according Ö 9 current

A COLUMN TO THE PARTY OF THE PA

equations: According Ç the third condition, among the 2 m

$$x^2 \equiv g_i \mod n$$
 (2)
 $x^2 \equiv g_i \mod n$ (3)

gi mod n

integers modulo n. at least one of them can be solved in x in the ring of

5

15 10 and/or the parameters of the Chinese remainders of the prime device private values comprises form of especially in a nomad object which, for example, takes the factors Said Q_i and/or f.m components $Q_{i,j}(Q_{i,j} \equiv Q_i \text{mod } p_j)$ of the also comprises: values Qi and of the public exponent v. The witness and/or the public modulus n and/or the m private a microprocessor-based bank card. a memory system comprises zone containing the f prime factors pi a witness The witness device device, contained

random value production means of the witness device random value production means hereinafter called

computation of commitments computation means, hereinafter called means R of the witness device. for the

20 commitment is commitments The means of computation make it possible to compute R in the computed ring of integers modulo

 either by performing operations of the type mod n

25 factor production means, r being such that 0 < r < n. where r is a random value produced by the random

 or by performing operations of the type $R_i \equiv r_i^{\vee} \mod p_i$

Chinese random collection of random values $\{r_1, r_2, ..., r_t\}$, produced by the where p_i such that $0 < r_i < p_i$, each r_i belonging factor production means and then by applying remainder method. r_i is a random value associated with the prime to

30

The witness device also comprises:

reception of the challenges d of the witness device, to integers or more challenges d; each challenge d comprising reception means hereinafter called the means for the di hereinafter called elementary challenges. receive 3

computation on the basis of each challenge d, of a response computation of the responses D of the witness device, computation means, hereinafter called means for for the

• either by carrying out operations of the type: $D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot ... \cdot Q_m^{dm} \mod n$

or by carrying out operations of the type:

10

5

 $D_i \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2}$ \cdots $Q_{i,m}^{dm}$ mod p_i

transmit and then by applying the Chinese remainder method one witness device also comprises or more commitments R and transmission means to one or more

responses numbers of the R, d, Ŭ. Q proof of the authenticity of an entity D forming a triplet referenced {R, d, D}. as there There are are as many responses D as commitments ₽. Each there group

called a demonstrator to an entity called a controller. Said system is such that it comprises a demonstrator

the invention is designed to prove the authenticity of an entity

In a first variant of embodiment, the system according to

a microprocessor in a microprocessor-based bank card. by interconnection means. It may especially take the form demonstrator device logic microcircuits in a nomad object, for example the form of associated is interconnected with the witness device with a demonstrator entity. οf

25

20

15

electromagnetic, optical or acoustic connection, device comprises demonstrator the the form of a terminal or remote Said system also comprises a controller device associated controller entity. Said controller device especially computer device. connection means communications server. for network, its Said controller electrical, especially Ö

Said system is used to execute the following steps:

35

30

act of commitment R

commitment R by applying the process specified above. part of each commitment R to the controller device through the device device transmit all or part of each commitment R to the demonstrator called the transmission means of the witness device, to witness device commitments transmission means of the demonstrator, to transmit all or connection means. At each also comprises through the interconnection comprises means R of the call, the transmission means, means witness device of transmission, ofmeans. computation The demonstrator hereinafter compute hereinafter of called each The

• Step 2: act of challenge d

15

10

S

20 challenges d to the demonstrator through the connection number of commitments R. The comprises commitment R, of the challenges means for the production, after receiving all or part of each transmission The controller device transmission means of the controller, means, comprises challenge d equal in number to hereinafter controller ťo transmit device called production also the the the

Step 3: act of response D

device receive each challenge d coming from the demonstrator specified above. the responses D from the challenges d by applying the process computation of the responses D of the device The means of reception of the challenges d of the witness through the interconnection means. witness device compute The means of

25

Step 4: act of checking

30

comprises: each response D to the transmission means of controller. the The controller device demonstrator transmit also

means of the controller device, computation means, hereinafter called the computation

means of the comparison means, hereinafter controller device. called the comparison

each First commitment case : the demonstrator has transmitted a part of

commitment R' satisfying a relationship of the type: from each challenge d and each response D, this reconstructed $G_1, G_2, ... Gm$, compute transmitted a part of each commitment R, the computation If the of the transmission means of the demonstrator have controller a reconstructed commitment device, having m public values

 $R' \equiv G_1^{dl} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \mod n$

or a relationship of the type:

10

S

 $R' \equiv D^{v}/G_1^{d1} \cdot G_2^{d2}$ $\ldots \ G_m{}^{dm} \ mod \ n.$

15 commitment R received. each reconstructed commitment R' with all or part of each The comparison means of the controller device compare

totality Second case : the demonstrator of each commitment R has transmitted the

20 computation ascertain controller transmitted the type: If the that each commitment R satisfies device, having m public transmission the totality means and the means of the demonstrator of each commitment comparison values a relationship G_1 , G_2 , means 0f have the the

 $R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^{\vee}$ mod n

25

30

35

or a relationship of the type: $R \equiv D^{\nu}/G_1^{dl} \cdot G_2^{d2} \cdot ...$

 \dots $G_m^{dm} \mod n$

Case of the proof of the integrity of a message

controller of the integrity of a message M associated with an combined invention is designed to give proof to an entity, known as a demonstrator comprises In a second known as a demonstrator. Said system is with the demonstrator variant embodiment first one, the system Said device demonstrator associated capable of being according to the such that it device with the

communications network, to the demonstrator device. connection means for its electrical, electromagnetic, optical or entity. Said controller device especially takes the a nomad object, for example in the form of a microprocessor interconnected terminal or remote comprises microprocessor-based bank card. It may especially take the form of logic microcircuits in connection, especially a controller device with the server. Said controller device witness device associated through with the by interconnection ย Said system data-processing form of a comprises controller

S

Said system is used to execute the following steps:

0

· Step 1: act of commitment R

transmission means of the commitment R by applying through the interconnection means. part witness commitments of each commitment At each device has means R of the call, the means of transmission, witness the process specified above. witness R to the demonstrator of computation device, device hereinafter to transmit compute of device all or called each The the

· Step 2: act of challenge d

20

15

device. The controller device also has challenge production each token T through the connection means to the controller transmission means of the demonstrator device, to transmit comprises compute at least one token T. The demonstrator device are the message demonstrator, applying hereinafter through the controller, commitments The demonstrator device comprises for the production, after having received the challenges d in a number equal to the hereinafter called to transmit the transmission means, hereinafter connection called the R. The controller device also has transmission M and all or part of each commitment a hashing function h whose arguments means. challenges d to the demonstrator the computation transmission computation means means means known number token ofof $\mathbf{a}\mathbf{s}$ Rto also the

25

30

• Step 3: act of response D

computation of the responses D of the the responses D from the challenges d by applying the process device receive each challenge d coming from the demonstrator specified above. The means of reception of the challenges d of the through the interconnection witness device compute means. The means witness

S

· Step 4: act of checking

10 15 this reconstructed commitment R' satisfying a relationship commitment R', from each challenge d and each response each response D to the controller. values computation comprises type: The $G_1, G_2, ..., G_m, to$ transmission computation means of the controller device, having m public means of means, firstly compute the demonstrator The controller device hereinafter a reconstructed called transmit the D,

 $R' \equiv G_1^{di} \cdot G_2^{d2} \cdot \dots G_m^{dm} \cdot D^v \text{ mod } n$

or a relationship of the type:

 $R' \equiv D^{v}/G_1^{dl} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \mod n$

20 all or part of each reconstructed commitment R'. the hashing function h having as arguments the message M and and then, secondly, to compute a token T' by applying

25 token T. device, to compare the computed token T' with the hereinafter The controller known as the comparison means of the controller device also has comparison received means,

authenticity Digital signature of a message and proof Of its

entity called a signing entity. the invention is designed to prove other of the first two embodiments, the invention, capable message In a third variant of an embodiment according M, hereinafter known as of being combined with one a signed the digital signature system according message, by an and/or to the the t o

The signed message comprises:

35

- the message M,
- the challenges d and/or the commitments R
- the responses D.

Signing operation

S

microprocessor in a microprocessor-based bank card. means and may especially take the form of logic microcircuits interconnected associated with the Said system is such that it comprises nomad with the object, signing entity. Said signing device for example witness device in by interconnection the a signing device form

Said system is used to execute the following steps:

· Step 1: act of commitment R

witness device comprises means of transmission, called the transmission means of the witness device transmit all or part of each commitment R to commitment R by applying the process specified commitments At each through the interconnection means. R of the call, the means witness of computation device compute the signing above. The hereinafter device, \mathbf{of} the t o

Step 2: act of challenge d

20

15

10

message M and all or part of each commitment R to compute device, applying a hashing function h whose arguments whose number is equal to the number of commitments hereinafter called binary The train and extract, from this binary train, challenges signing the computation device comprises means of the computation 77 . are signing means,

Step 3: act of response D

25

the responses D from the challenges d by applying the process signing device through the interconnection means. The means means, hereinafter called means of transmission of the witness for computing witness device receive each challenge d means for the reception of the challenges d of the above. the responses D of the witness device compute The witness device comprises coming transmission from the

through the device, to transmit the responses interconnection means. U ō the signing device,

Checking operation

S

known as the controller checks the signed message. To prove the authenticity of the message M, an entity

electromagnetic, optical or acoustic device. through a computer communications network, to the signing takes the form of a terminal or remote server. with the Said system comprises a controller comprises controller connection entity. Said controller device means connection, for device its Said controller associated especially especially electrical,

transmission means of the message comprising: connection comprises Said signing device controller means. Thus transmission device, the controller signing means, associated with the of the signed message device, for the transmission, hereinafter device has known signing entity through the a signed as the

15

10

the message M,

20

- the challenges d and/or the commitments R,
- the responses D.

The controller device comprises:

- means of the computation means hereinafter controller device, called the computation
- 25 means of the controller device. comparison means, hereinafter called the comparison
- commitments R, challenges d, Case where the controller responses device has
- challenges responses controller If the controller device has commitments R, challenges d, D, the computation and comparison means d and the responses device ascertain that the D satisfy relationships commitments of the of the the

 $R \equiv G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \cdot D^v \mod n$

or relationships of the type:

35

 $R \equiv D^{v}/G_1^{dl} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \mod n.$

controller device ascertain that the message M, the challenges d and the commitments R satisfy the hashing function: Then, the computation and comparison means of the

d h(message, \mathcal{R}

S

and responses Case where Ū the controller device has challenges

satisfying relationships of the type $R' \equiv G_1^{dl} \cdot G_2^{d2} \cdot ... \cdot G_m^{dm} \cdot D^v$ of each challenge d and computation means of the controller reconstruct, on the basis If the controller has challenges d and responses D, the each response D, commitments

10

mod n

15

or relationships of the type: $R' \equiv D^{v}/G_1^{dl} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \mod n.$

controller challenges Then the computation and d satisfy the hashing function: device ascertain that the message comparison means of M and the the

<u>а</u> П h (message, R')

and responses D Case where the controller has commitments Z

20

25

apply the hashing function and compute d' such that: responses If the controller D, the computation means of the controller device device has commitments R and

d' = h (message, R)

controller challenges d' and the responses D satisfy relationships the computation device ascertain that the and comparison means commitments ofof the the the

 $R \equiv G_1^{d'1} \cdot G_2^{d'2}$ $\ldots \ G_m{}^{d^*m} \ . \ D^v \ mod \ n$

or relationships of the type: $R \equiv D^{v}/G_1^{d^{11}} \cdot G_2^{d^{12}} \cdot ... \cdot G_m^{d^{1m}}$

30

mod n

Device

35

a nomad object, for example the form of a microprocessor in with an entity. The terminal device especially takes the form of The invention also relates to a terminal device associated

designed to prove the following to a controller device: microprocessor-based bank card, The terminal device

- the authenticity of an entity and/or
- the integrity of a message M associated with this entity.

following parameters or derivatives of these parameters: This proof is established by means of all or part of the

S

- Gı, G₂, ... G_m (m being greater than or equal to 1), - m pairs of private values Q₁, Q₂, ... Q_m and public values
- factors $p_1, p_2, \dots p_f$ (f being greater than or equal to a public module n constituted by the product of f prime

10

related by relationships of the type Said module and said private and public values

 $G_i \cdot Q_i^{\mathsf{v}} \equiv 1 \mod n \text{ or } G_i \equiv Q_i^{\mathsf{v}} \mod n$

designating a public exponent of the type $y = 2^k$

15

 $v = 2^k$

where k is a security parameter greater than 1.

numbers $g_1,g_2, ... g_m$ being produced such that ... p_f ; said f prime factors p_1 , p_2 , ... p_f and/or base numbers conditions Said m public values G_i are the squares g_i^2 are satisfied. g₁,g₂, ... g_m inferior to the f prime factors p₁, p₂, the following of m distinct said m base

First condition

20

According to the first condition, each of the equations: $x^{v} \equiv g_{i}^{2} \mod n \quad (1)$

Second can be solved in x in the ring of integers modulo n condition

25

 $G_i \equiv$ Qi to the square modulo n, k-1 times, one of them is different from Q $\pm g_i$ (that is to say non trivial). According to the second condition, in the case where mod n, among the m numbers qi obtained by raising

times, one of them trivial). raising the $G_i \cdot Q_i^{\mathsf{v}}$ According to the second condition, in $\equiv 1 \mod$ inverse of Q_i modulo n to the square n, is different from $\pm g_i$ (that among the m numbers the case where qi obtained modulo n, is to say non ЬУ

35

notation ±gi represents the numbers is pointed out here that g_i and n-g_i. according ō þ current

Third condition:

Ø

equations: According ō the third condition, among the 2 m

$$x^2 \equiv g_i \mod n$$
 (2)
 $x^2 \equiv g_i \mod n$ (3)

integers at least one of them can be solved modulo n. i × in the ring o f

15 10 and/or the parameters of the Chinese remainders of the prime comprising private values Qi and of the public exponent v. values Q_i and/or f.m components $Q_{i,j}$ ($Q_{i,j} = Q_j \mod p_j$) of the factors Said terminal and/or the public modulus n and/or the m private a memory device zone containing the f prime comprises 2 witness device factors pi

he witness device also comprises:

- random value production means of the witness random value production means hereinafter device. called
- 20 computation of commitments R of the witness device rıng of the integers modulo n. - computation means, hereinafter called means for the in the

Each commitment is computed

• either by performing operations of the type:

$$R \equiv r^{v} \mod n$$

- 25 production means, r being such that 0<r<n. where r is a random value produced by the random value
- or by performing operations of the type:

 $R_i \equiv r_i^{\ v} \ mod \ p_i$

number p_i such that $0 < r_i < p_i$, each r_i belonging to a collection production of random method. where ri is a random value associated with the prime means, then by applying the values $\{r_1, r_2, ..., r_f\}$ produced by the random value Chinese remainder

30

The witness device also comprises:

integers di hereinafter called elementary challenges; reception of the challenges d of the witness device, to receive or more challenges d, - reception means hereinafter called the means for the each challenge d comprising

U, computation, on the computation computation of the responses D of the witness device, for the means, hereinafter called basis of each challenge d, of a response means for the

• either by performing operations of the type:

 $D \equiv r \cdot Q_1^{d1} \cdot Q_2^{d2} \cdot \dots \cdot Q_m^{dm} \mod n$

10

S

or by performing operations of the type: $D \equiv r_i \cdot Q_{i,1}^{d1} \cdot Q_{i,2}^{d2} \cdot ... \cdot Q_{i,m}^{dm} \mod p_i$

and then by applying the Chinese remainder method

15 to transmit one or more challenges responses numbers R, d, D forms a triplet referenced {R, d, D}. Said witness device D. There are as many responses Д as there are commitments R. Each also comprises commitments R and one or more transmission means D as there group are

according Case of the proof of the authenticity of an entity In a first embodiment variant, the to the invention is designed to terminal device prove the

20

called a controller. authenticity of an entity called a demonstrator to an entity

25

demonstrator device associated with device by interconnection means. It may especially take Said demonstrator device is interconnected with the witness form of logic microcircuits in a nomad object, for example the of a microprocessor in a microprocessor-based bank Said terminal device is such a demonstrator that it comprises entity.

means for its electrical, communications connection, Said demonstrator especially network, device also comprises electromagnetic, to the controller device through optical data-processing connection or acoustic associated

the the form controller of a terminal or remote entity. Said controller device server. especially

steps: Said terminal device is used to execute the

· Step 1: act of commitment R

S

commitment R by applying the process specified above commitments At each R of the call, the means witness of device computation compute each the

15 10 device transmit all or part of each commitment R to the demonstrator hereinafter called transmission means of the witness device, to part of each commitment R to the controller device, through transmission means device connection means through the interconnection means. The demonstrator also has transmission means, hereinafter called witness of the demonstrator, to device has means of transmission, transmit all or the

response Steps 2 and 3: act of challenge d, act

challenges d by applying the process specified above the witness device. The means of computation of the responses interconnection means device device D of the witness device compute the The means of reception of the challenges d of the witness and the demonstrator through the connection means between receive each challenge d coming from between the demonstrator device device responses and through the the controller U controller from the and the

Step 4: act of checking

25

20

check. response D to the controller device that carries The transmission means of the demonstrator transmit

Case of the proof of the integrity of a message

30

35

entity, known according to the invention is designed combined In a second with the first embodiment, as a controller, embodiment of the integrity variant to give proof the capable terminal ofa message ofdevice to being

demonstrator device being interconnected device associated terminal device associated with communications network, to the controller form of logic microcircuits in a nomad object, for example the device connection, card. takes the form of a terminal or remote server. the Said demonstrator device comprises connection means of a microprocessor in a microprocessor-based by interconnection electrical, controller especially an entity known is such entity. Said controller device with electromagnetic, that it comprises means. It may especially take the demonstrator through as a demonstrator. optical อ device with the ಬ data-processing demonstrator entity, or associated especially acoustic witness bank

steps Said terminal device is used to execute the following

· Step 1: act of commitment R

15

10

5

or part of each commitment R to the demonstrator device witness device has means of transmission, hereinafter called commitment R by applying the process specified above. commitments transmission means of the witness device, to transmit all At each the interconnection means. R of call, the means the witness of computation device compute of each The the

20

response Steps 2 and 3: act of challenge act o f

are the message M and all or part of each commitment R, to demonstrator, applying each token T, through the connection means, to the controller transmission compute hereinafter The demonstrator device comprises transmission at least one token T. The demonstrator device means called the of the means, a hashing function h whose arguments demonstrator computation hereinafter computation means device, means known to transmit of $\mathbf{a}\mathbf{s}$ also the

30

produces challenges commitments R Said controller device, after having received the token d in a number equal to the number

the witness device. The means of computation of the responses interconnection means between the demonstrator device device through the interconnection challenges d by applying the process specified above D of the witness device controller device device The means of reception of the challenges d of the witness receive each challenge d coming from the controller and the demonstrator device and through compute the responses D from the means between and

Step 4: act of checking

10

Ŋ

authenticity Digital The transmission means of the demonstrator send each signature D to the controller device which performs the check. of a message and proof of its

15

signature combined with either one of the first two, message, by an entity called a signing entity. according a third embodiment variant, of a message M, hereinafter known as to the invention is designed to produce capable the terminal the the of device signed digital being

The signed message comprises:

20

- the message M,
- the challenges d and/or the commitments R
- the responses D.

25

a nomad object, fox example the form of a microprocessor in means. It may especially take the form of logic microcircuits in interconnected with the device associated with the signing entity. Said signing device is comprises through a data-processing electromagnetic, controller microprocessor-based Said terminal device is such that it comprises device connection optical associated witness or bank card. Said signing device communications means acoustic with the device by interconnection connection, for controller network, to entity. especially a signing electrical,

30

controller device especially takes server. the form ofþ terminal o r

Signing operation

S

steps: Said terminal device is used to execute the following

· Step 1: act of commitment R

witness device comprises means commitment R by applying the process specified transmit all or part of each commitment called the commitments device through the interconnection means. At each transmission means of the witness R of the call, the means witness device of transmission, of computation R to compute the hereinafter device, of signing each

10

Step 2: act of challenge d

15

a binary train and extract, from this binary train, challenges d message M and all or part of each commitment R, to compute whose number is equal to the number of commitments R. device, applying a hashing function h whose arguments hereinafter The signing called device comprises computation the computation means of the are means,

Step 3: act of response D

20

called means of transmission of the witness device, to transmit The witness device comprises transmission means, hereinafter from the challenges d by applying the process specified above responses D of the witness device compute each challenge interconnection interconnection responses The means for the reception of the challenges d receive d coming means. The means for computing the means. D to from the signing device through the the signing device, through the responses

25

Controller device

30

35

controller device may especially take the form of controller remote The invention also relates server device associated is designed to check: with a controller ō a controller a terminal or device. entity.

- the authenticity of an entity and/or

the integrity of a message M associated with this entity.

following parameters or derivatives of these parameters: - m pairs of public values $G_1,\,G_2,\,...\,G_m$ (m being greater This proof is established by means of all or part of the

than or equal to 1),

S

unknown to the controller device and the associated controller entity. prime factors $p_1, p_2, ..., p_f$ (f being greater than or equal to 2), a public modulus n constituted by the product of f

related by relationships of the type Said modulus and said private and public values

 G_i . $Q_i^{\ v} \equiv 1$. mod n or $G_i \equiv \ {Q_i}^{\ v}$ mod n

v designating a public exponent of the type:

 $v = 2^k$

15

10

where k is a security parameter greater than 1.

numbers $g_1, g_2, \dots g_m$ being produced such that the following base numbers $g_1, g_2, ... g_m$ inferior to the f prime factors $p_1, p_2,$... pf; said f prime factors conditions Said m public values G_i being the squares $g_i^{\ 2}$ of m distinct are satisfied. p₁, p₂, ... p_f and/or said m base

First condition

20

According to the first condition, each of the equations: $x^v \equiv g_i^2 \mod n$ \odot

can be solved in x in the ring of integers modulo n

Second condition

25

30

different from ±g_i (that is to say non trivial). Q_i to the square modulo n, k-1 rank times, one of them is $G_i \equiv Q_i^{v}$ According to the second condition, in the case where . mod n, among the m numbers qi obtained by raising

rank times, one of them is different from ±gi (that is to raising the inverse of Qi modulo n to the square $G_i \cdot Q_i^{\vee} \equiv 1 \mod n$, trivial). According to the second condition, in among the m numbers the case where qi obtained modulo n, k - 1

notation ±gi represents the numbers is pointed out here that gi and n-gi. according Ö ಣ current

Third condition

S

According to the third condition, among the 2 m

 $x^2 = g_i \mod n$ (2) $x^2 = g_i \mod n$ (3)

integers modulo n. at least one of them can be solved in x in the ring of

10 Case of the proof of the authenticity of an entity

authenticity of an entity called a demonstrator and an entity according In a first embodiment variant, the controller device controller. to the invention is designed to prove the

15 Ö especially through a data-processing communications network, its electrical, electromagnetic, optical or acoustic connection, entity. a demonstrator device associated with the demonstrator Said controller device comprises connection means for

20 steps: Said controller device is used to execute the following

challenge Steps 1 and .. act of commitment

ofdemonstrator device all or part of the commitments R Said controller device also has means for the through the connection means. coming from the reception

25

integers commitment R, of the challenges d in a number equal to the number The controller for the di hereinafter called of commitments R, each challenge production, after receiving device comprises challenge production elementary challenges. all or part of each d comprising

through the controller, The hereinafter to transmit the challenges d to the demonstrator controller connection means. called device transmission also comprises means transmission of

35

checking W 4: act Of: response Ų, act 0

The controller device also comprises:

from the - means for the reception demonstrator device, through the connection means, of the responses U coming

S

- means of the computation means, hereinafter called the computation controller device,
- means of the controller device. comparison means, hereinafter called the comparison
- part of each commitment R. First case: the demonstrator has transmitted

10

of the controller device, having m public values satisfying a relationship of the type: $R' \equiv G_1^{d1} \cdot G_2^{d2} \dots G_m^{dm} \cdot D^v \mod n$ compute a reconstructed commitment R', from each challenge received a part of each commitment R, the computation means and each response D, If the reception means this reconstructed commitment of the controller device have $G_1, G_2, \ldots G_m,$

15

or 8 relationship of the type:

20

 $R' \equiv D^{v}/G_1^{d1} \cdot G_2^{d2} \cdot ... \cdot G_m^{dm} \mod n.$

commitment R reconstructed commitment R' with all or part The comparison means of the controller device received. compare of each

the totality of each commitment Second case: the demonstrator **⊼** has transmitted

25

30

commitment R satisfies a relationship of the $R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot ... G_m^{dm} \cdot D^v$ received the totality of each commitment R, the computation having If the m public values G₁, G₂, ... G_m, ascertain that and the reception comparison means of the controller means of the controller device have type: device,

mod, n

۵ relationship of the type: $R' \equiv D^{v}/G_1^{d1} \cdot G_2^{d2}$ G_m dm mod n.

Case of the proof of the integrity of a message

combined associated invention a with the first, the controller device with an entity known as a demonstrator. is designed to second embodiment prove the variant capable integrity of a message according to the being

ō its electrical, electromagnetic, entity. especially through a data-processing communications network, a demonstrator Said controller device comprises connection means device associated optical or acoustic connection, with the demonstrator

Said controller device S used ō execute the following

challenge Steps ۵ and 2: act of commitment ₹, act o f

15

10

S

25 20 challenges hereinafter called elementary challenges. The controller device of commitments the token T, of challenges production connection means. transmission Said controller device has T coming Q means for the means. The transmission to the means R, each challenge from demonstrator of the the d in a number equal to the number controller means, production, demonstrator has means for the controller, d comprising through the hereinafter device after having device Ö has challenge transmit m integers reception through called connection received

hecking Steps w and 4: act of response D, act o f

computation means of the controller also comprises device, through reception of the responses commitment R', from each challenge values Said controller device also comprises means G₁, G₂, ... G_m, to first of all compute computation means, the connection means. D coming from the demonstrator device, d and each response hereinafter called the Said controller device having a reconstructed B for public

type: reconstructed commitment R' satisfying a relationship o f

 $R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot ... G_m^{dm} \cdot D^v \mod n$

S

or a relationship of the type: $R' \equiv D^{V}/G_1^{d1} \cdot G_2^{d2} \cdot ... \cdot G_m^{dm} \mod n$

or part of each reconstructed commitment R'. hashing function h having as arguments the message and then, secondly, to compute a token T' by applying M and all

10 device to compare the computed token T' with the token T. hereinafter called the The controller device comparison means also has comparison of the controller received means,

authenticity Digital signature of a message and proof of

20 15 embodiments, the controller device according to the invention combined with either checking a signed message by means of an entity called a is designed to prove the authenticity controller. a third embodiment one or the variant, capable other of the of the message of being first two

comprises: a signing entity having a hashing function h (message, R) The signed message, sent by a signing device associated

the message M,

25

- the challenges d and/or the commitments **7**7,
- the responses D.

Checking operation

device, through the controller device receives the signed message from the signing especially through a data-processing communications its electrical, electromagnetic, optical or acoustic connection, signing device Said controller device comprises connection means connection means. associated with the signing entity. Said network, for

30

The controller device comprises:

- means of the controller device, computation means, hereinafter called the computation
- means of the controller device. comparison means, hereinafter called the comparison
- commitments R, challenges d, Case where the responses D controller device has

S

challenges controller responses If the controller device has commitments R, challenges d, D, the computation and comparison means d and the responses D satisfy relationships device ascertain that the commitments ₹, of the of the the

$$R \equiv G_1^{d1} \cdot G_2^{d2} \cdot ... G_m^{dm} \cdot D^v \mod n$$

15

10

or relationships of the type:

$$R \equiv D^{\nu}/G_1^{d1} \cdot G_2^{d2} \cdot \dots G_m^{dm} \mod n.$$

controller device ascertain that the message M, the challenges d and the commitments R satisfy the hashing function: Then the computation and comparison means of the

$$d = h$$
 (message, R)

d and responses D: Case where the controller device has challenges

20

commitments R' satisfying relationships of the type: the computation means of the controller device basis of each If the controller device has challenges d and responses challenge d and each response D, compute can, on the D,

 $R' \equiv G_1^{d1} \cdot G_2^{d2} \cdot ... G_m^{dm} \cdot D^v \mod n$

or relationships of the type:

25

$$R' \equiv D^{v}/G_1^{d1} \cdot G_2^{d2} \cdot \dots \cdot G_m^{dm} \mod n$$

challenges d satisfy the hashing function controller and then the computation and comparison device ascertain that the message means of the M and the

= h(message, R')

30

commitments Case Z where and responses controller J device has

apply the hashing function and compute d' such that responses D, the computation controller device has means of the controller device commitments R and

d'= h (message, R)

type challenges controller and then the computation d' and device the ascertain that the commitments responses D satisfy relationships and comparison means ofOf. the the the

 $R \equiv G_1^{d'1} \cdot G_2^{d'2} \cdot ... G_m^{d'm} \cdot D^v \mod n$

or relationships of the type:

10

S

 $R \equiv D^{v}/G_1^{d'1} \cdot G_2^{d'2} \cdot \dots \cdot G_m^{d'm} \mod n$

Description of the invention

20 15 corresponding public number or numbers. The proving entity several private numbers. Another entity checks; it knows the transfer of knowledge". An entity proves that it knows one digital signature of messages. These are methods authentication of entities and private number or numbers, in such a way as to be able to use as many times as needed. The goals to convince the checking entity without revealing the of the GQ methods messages are together the "without," with the dynamic 0 T

of secret high prime numbers. A public exponent ν and a public modulus n together form a verification key $\langle \nu, n \rangle$ number Q together form a pair of numbers type, direct: $G \equiv Q^{\nu} \pmod{n}$ or inverse $GxQ^{\nu} \equiv I \pmod{n}$. means of one meaning "raise to the power ν modulo n" and implement by public modulus n together form $\{G,Q\}$ for the same key $\langle v,n \rangle$. each GQ method implements one generic equation linked to a public number G and a private within the checking entity, but not within the proving entity; in The type the security analyses confound the Each GQ method depends on a public modulus composed has an effect on the operation of the calculations or several generic or several equations, all of the same $\{G,Q\}$. To resume two types. pairs of numbers

30

100

identification data and this proof does not reveal the signature an RSA signature single pair of numbers $\{G,Q\}$: the public number G is deduced uses an RSA digital signature technology. The private number Q or its inverse modulo n is from identification data according to a format mechanism preferably a prime number. Each GQ1 method in general uses a needed. which therefore $<\nu,n>$ is then an RSA public key where the odd exponent ν is A classic version of the GQ method, here called GQL an integral part of the RSA digital signature knowledge remains secret, to be used as many times as for identification data. of an RSA signature mechanism. The verification The proving of its

0

S

30 25 20 15 "identity based". Thus, an emitter of chip cards uses his RSA other by identification data. Such accrediting or clients in session, know an RSA his RSA private key when entering each session to calculate a card; or furthermore, a client on a network of computers number Q which is inscribed as diversified private key in the private key for the emission of each card to calculate a private keys: the RSA private signing key is reserved for an authority modulo result for each of the prime entity to use the Chinese remainder factors at the level of each entity, almost the modulus of 768 identification data; they do not know the RSA private private number Q which will be the ephemeral private key of Nonetheless, which, in the client during the session. The proving entities, chip The GQ1 methods generally implement two levels of by RSA with a modulus of 512 bits with three prime entities distinguishing same dynamic authentication of entities by GQ1 with a key hierarchy, is at the next higher level. bits at the level of an authority requires work load as a dynamic a mechanism is said to be themselves which allows technique by calculating a factors before calculating signature authentication one the from ofproving cards the

35

modulo result for their product.